#01 09 15

SONDER-AUSGABE

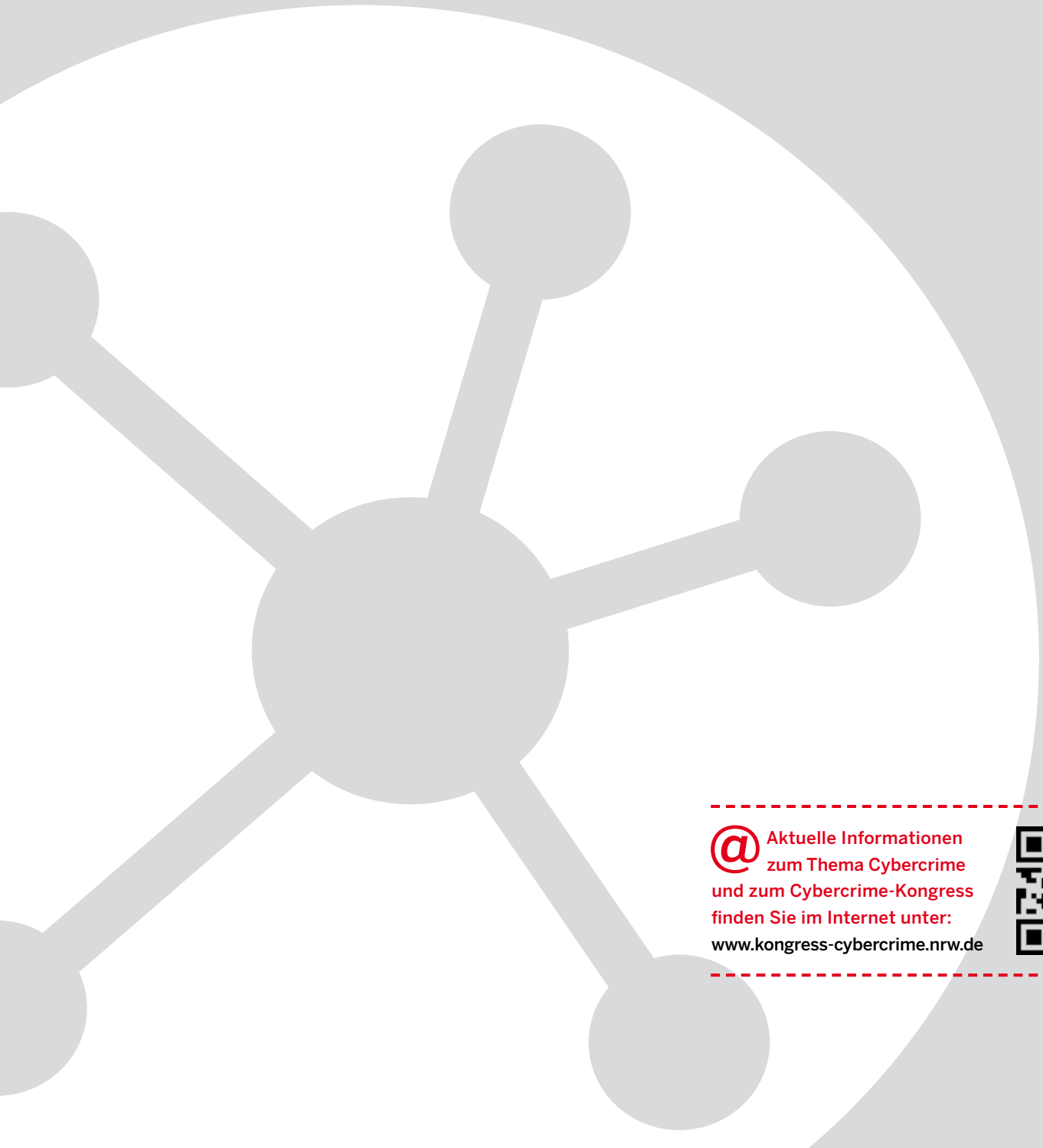
Streife

Das Magazin der Polizei des Landes Nordrhein-Westfalen

CYBERCRIME Die Polizei NRW im Kampf gegen Computerkriminelle

»Wir sind auf dem Weg zur Smart-Polizei.«

Ralf Jäger MdL
Innenminister des Landes Nordrhein-Westfalen



@ Aktuelle Informationen zum Thema Cybercrime und zum Cybercrime-Kongress finden Sie im Internet unter:
www.kongress-cybercrime.nrw.de

Ralf Jäger MdL

Innenminister des Landes
Nordrhein-Westfalen

Liebe Leserin, lieber Leser,

in meiner Jugend hatten nur eine Handvoll Menschen einen Computer – und heute? Stellen Sie sich heute Jugendliche ohne Smartphone vor. Undenkbar, oder? Computer haben die Welt verändert, und sie werden es auch zukünftig tun. Sie erleichtern Ihnen und mir den Alltag, sie erinnern an Geburtstage und ermöglichen auf die Schnelle auch gleich den Online-Kauf eines Geburtstagsgeschenks, wenn die Zeit knapp ist. Computer und deren allgegenwärtige Vernetzung erleichtern aber auch den Straftätern das Leben. Ständig tauchen neue »digitale Kriminalitätsphänomene« auf. Manche Delikte, wie die Verbreitung kinderpornografischer Schriften, finden fast nur noch in der digitalen Welt statt.

Mit dieser Sonderausgabe nehmen wir Sie auf eine spannende Reise durch die vielfältigen Aufgaben unserer Polizei bei der Bekämpfung der digitalen Kriminalität mit. Auf dieser Reise können wir Ihnen hoffentlich auch Berührungsängste und Vorbehalte nehmen. Sie werden feststellen, dass wir alle in der Polizei heute schon tagtäglich Berührungspunkte zur sogenannten Cybercrime haben. Smart-Home und salafistische Internetpropaganda sind nur zwei Begriffe, die exemplarisch die nützlichen und gefährlichen Seiten des Internets verkörpern.

Ständig aufs Neue stellt sich die Frage, ob wir im Katz-und-Maus-Spiel zwischen Polizei und Straftätern gut aufgestellt sind. Derzeit kann ich das bejahen, denn wir haben rechtzeitig unsere Organisation, die Zuständigkeiten sowie die Aus- und Fortbildung an moderne, digitale Aufgaben angepasst. Da der Cyberspace auch aus dem dienstlichen Alltag nicht mehr wegzudenken ist, möchten wir der jungen, dynamischen Kollegin im Wachdienst ebenso wie dem »ergrauten« Sachbearbeiter im Ermittlungsdienst gleichermaßen die Kernkompetenzen für den Umgang mit den digitalen Herausforderungen der täglichen Polizeiarbeit vermitteln. Man könnte sagen, wir sind auf dem Weg zur Smart-Polizei.

Dennoch bleibt festzustellen, dass die Polizei nicht alleiniger Akteur bei der Bekämpfung der Cybercrime und beim Schutz der Bürgerinnen und Bürger vor Gefahren aus dem Internet sein kann. Die besten Chancen im Kampf gegen die Cybercrime bestehen, wenn wir als Polizei NRW vereint mit unseren Partnern handeln. So tragen beispielsweise die Kooperationen mit dem »Bundesverband der Informationswirtschaft, Telekommunikation und neue Medien« (Bitkom) sowie dem »Bundesverband der IT-Anwender« (VOICE) und der Fachhochschule Aachen dazu bei, innovative Ermittlungs- und Präventionsansätze zu entwickeln.

Schließlich enthält diese Sonderausgabe auch nützliche Tipps, die Sie davor bewahren, selbst Opfer krimineller Machenschaften zu werden. Denn jeder von uns kann Ziel von Cyber-Angriffen werden.

Bleiben Sie wachsam!

Ihr Ralf Jäger

INHALT

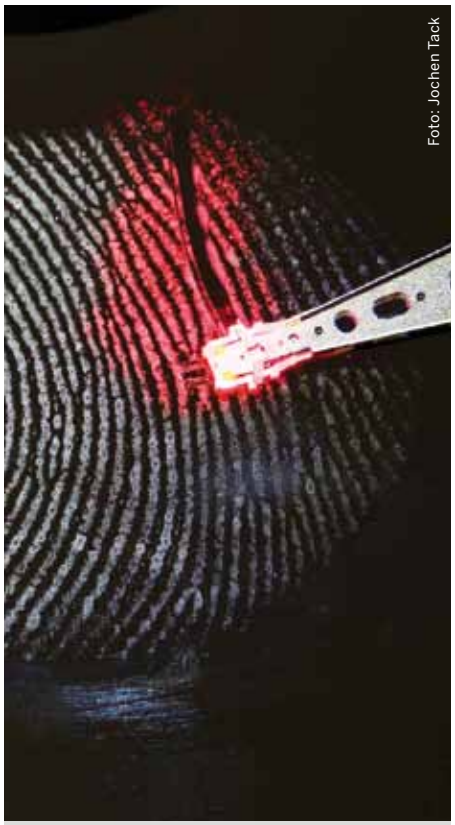


Foto: Jochen Tack

04 WAS IST CYBERCRIME – VON RANSOMWARE, SEXTING & TROJANERN


Foto: Oliver Krato

20 CYBERCRIME-KOMPETENZZENTRUM – AUFGABENBEREICHE & PERSONEN


Foto: Oliver Krato

30 SICHERHEITSKOOPERATIONEN – GEMEINSAM GEGEN CYBERCRIME

02 __ **Editorial**
43 __ **Impressum**
06 __ **Was ist Cybercrime?** Von Ransomware, Sexting und Trojanern
14 __ **Die wichtigsten Cybercrime-Phänomene**
18 __ **Landeskriminaldirektor Dieter Schürmann im Gespräch** »Wir brauchen digitales Denken für Ermittler und Einsatzkräfte«
20 __ **Das Cybercrime-Kompetenzzentrum** Die zentralen Aufgabenbereiche
22 __ **Wer steckt dahinter?** Die Experten des Cybercrime-Kompetenzzentrums
24 __ **Das Erfolgsmodell Cybercrime-Kompetenzzentrum** Der Direktor des Landeskriminalamtes Nordrhein-Westfalen im Gespräch
27 __ **Cybercrime und politisch motivierte Kriminalität** Islamistischer Terrorismus, Rechts- und Linksradikalismus im Netz
30 __ **»Gemeinsam gegen Cybercrime«** Vernetzt zum Erfolg
34 __ **International, anonym und gut verschlüsselt** Polizeiarbeit mit Hindernissen

Foto: Ralph Lueger

38 FORTBILDUNG BEIM LAFP – EINSTEIGER- & EXPERTENSCHULUNG

Foto: Jochen Tack

67 CYBERCRIME GESTERN & HEUTE – ÜBER DISKETTE & KASSETTENREKORDER

Foto: Jochen Tack

70 LÖTEN, FRÄSEN, SELBER BAUEN – DIE ARBEIT DER FORENSIK-EXPERTEN

38 __ **IT-Fortbildungen beim LAFP**
Von Einsteigerseminaren bis Expertenschulungen
42 __ **Präventionsfilme »Sichere Netzwelten«** Bewusstsein schaffen für Cybermobbing, Datenklau und Passwort-Phishing
46 __ **Einen Medienscout, bitte!**
49 __ **Angriffe aus dem Netz** »Wir tun alles, um Polizeidaten zu schützen«
52 __ **Optische Tarnkappen und intelligente Kochtöpfe** Zukünftige Entwicklungen im Cyberbereich
58 __ **»Big Data«** Die Polizei im Kampf gegen die Datenflut
62 __ **Handarbeit statt Softwareprogrammierung** Kooperation mit der Fachhochschule Aachen beschert Cybercrime-Kompetenzzentrum neuen Mitarbeiter
65 __ **Arbeiten im Cybercrime-Kompetenzzentrum** Eine hohe IT-Affinität ist Voraussetzung
67 __ **Als noch mit Diskette und Kassettenrekorder gearbeitet wurde** Cybercrime gestern und heute
70 __ **Löten, fräsen, selber bauen** Die Arbeit der Forensik-Experten im Cybercrime-Kompetenzzentrum

BEST PRACTICE

Was ist Cyber-crime?

Von Ransomware, Sexting und Trojanern

Cybercrime hat viele Gesichter – und es kommen immer mehr dazu. Denn die Täter sind kreativ und fleißig, wenn es um neue Angriffstechniken geht. Außerdem eröffnen neue Technologien auch immer neue Angriffsflächen. Die zunehmende Verbreitung etwa von Smartphones und Tablets bietet nicht nur Cyberkriminellen ein erweitertes Arbeitsfeld, sondern sie sorgt auch dafür,

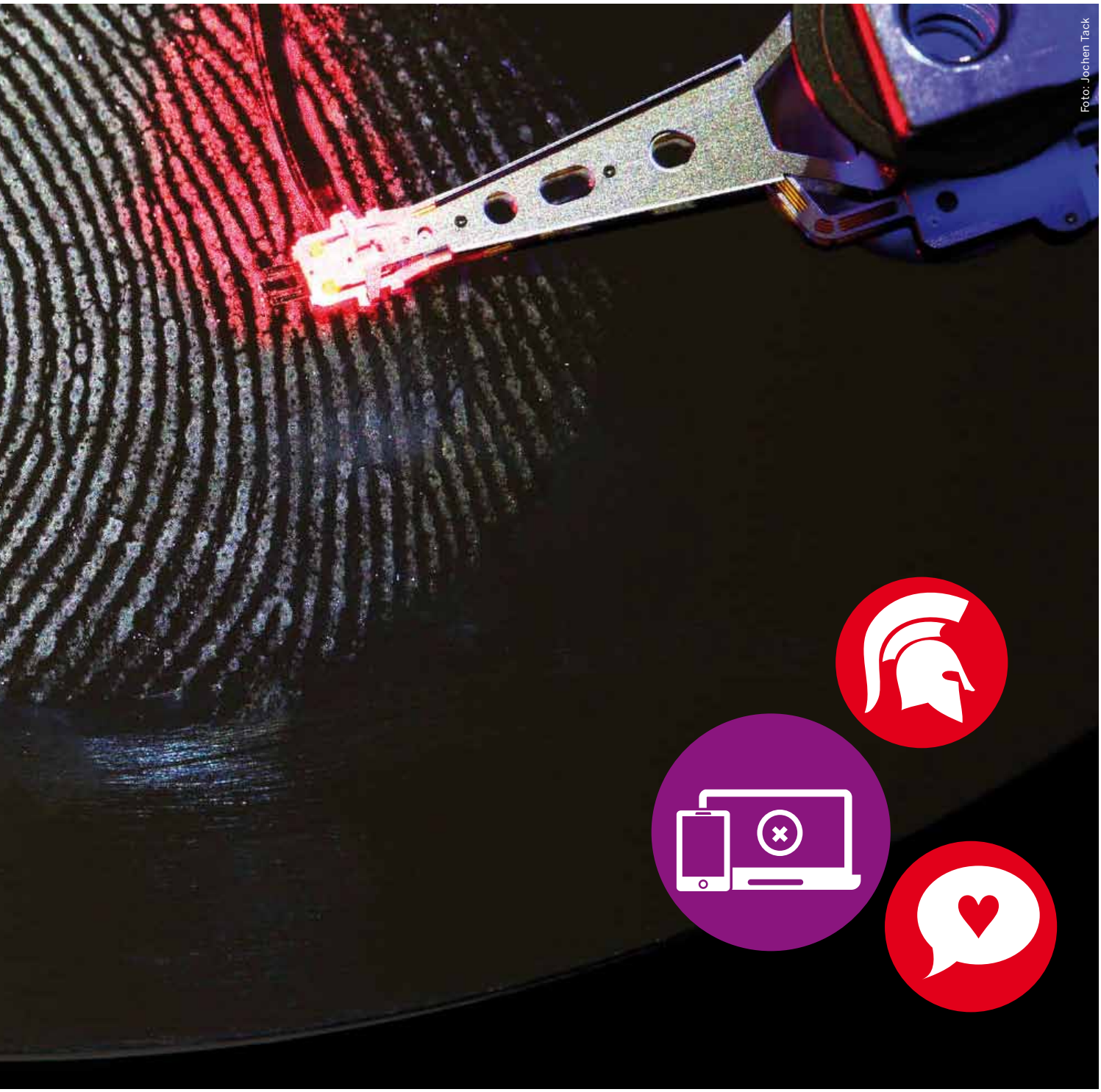


Foto: Jochen Tack

dass Phänomene wie Cybermobbing oder Sexting besonders unter Kindern und Jugendlichen zunehmen. Welche Cybercrime-Phänomene beschäftigen die IT-Experten und Präventionsbeamten in den Behörden am meisten? Die Kriminalhauptkommissare Lorenz Wüsten vom PP Bonn, Horst Radtke vom PP Duisburg und Michael Paech vom PP Essen geben Einblicke in ihre Arbeit. >

Foto: Julia Fischer

»Sie denken, sie verschenken ein Handy. Ein Smartphone ist aber kein Handy, sondern ein Computer.«

Lorenz Wüsten,
Fachmann des PP Bonn für Jugendmedienschutz

Lorenz Wüsten arbeitet in der Prävention im Bereich Cybercrime. Sein Schwerpunkt ist dabei der Jugendmedienschutz. Die Schulen im Bonner Raum melden sich in der Regel immer dann bei ihm, wenn es dort einen konkreten Vorfall gegeben hat – häufig gibt es Probleme mit Cybermobbing. »Die Situation hat sich in den vergangenen zwei Jahren noch einmal verschärft, da offensichtlich nicht nur Jugendliche, sondern auch viele Kinder Smartphones besitzen. Ich bekomme vermehrt Anfragen von Grundschulen, weil es dort bereits in den dritten und vierten Klassen Fälle von Cybermobbing gibt – das ist eine ganz neue Entwicklung«, erklärt Lorenz Wüsten. Problematisch sei, dass viele Eltern nicht abschätzen könnten, was es bedeutet, wenn sie einem zehnjährigen Kind ein Smartphone schenkten. »Die Eltern kennen sich häufig mit den Geräten nicht aus. Sie denken, sie verschenken ein Handy. Ein Smartphone ist aber kein Handy, sondern ein Computer, mit dem die Kinder alles machen können – vom Aufrufen von pornografischen Seiten über Online-Einkäufe, Chatten bis zum Erstellen von eigenen Nacktfotos inklusive dem anschließenden Versand über Messenger-Programme oder dem Hochladen in Soziale Netzwerke ist alles möglich.« Ziel ist es daher häufig erst einmal, die Eltern über mögliche Gefahren aufzuklären und auch die Lehrerinnen und Lehrer mit ins Boot zu holen. Denn wenn es schon bei den Erwachsenen an dem nötigen Bewusstsein für diese Problematiken fehlt, kann man dieses von den Kindern erst recht nicht erwarten.

Cybercrime-Prävention zunehmend auch Thema für Pädagogen

Unterstützung holt sich Lorenz Wüsten bei seinen Besuchen in den Schulen von einer Medienpädagogin – wenn es um das Thema Sexting geht, ist sogar eine Sexualpädagogin dabei. »Die Cybercrime-Prävention geht mittlerweile in Bereiche, die man als Polizist nicht mehr alleine bewältigen kann. Ich kann zwar darüber aufklären, was erlaubt und was verboten ist, ich bin aber kein Pädagoge mit einem Bildungs- oder Erziehungsauftrag. Besonders wenn wir jetzt vermehrt mit Kindern arbeiten, sollte die Präventionsarbeit daher pädagogisch begleitet werden«, so der Experte. Auch auf die Fragen der Eltern müsse adäquat reagiert werden, denn nachdem man über Probleme wie Cybermobbing, Sexting oder Online-Sucht aufgeklärt hätte, kommt häufig die Frage: »Und was mache ich jetzt?«. Dies zu beantworten, sei dann Aufgabe der Pädagogin. Fakt ist, dass viele Eltern völlig geschockt über die zum Teil exzessive Smartphone-Nutzung ihrer Kinder sind. Dabei ist es nicht ungewöhnlich, dass Jugendliche innerhalb einer Woche bis zu 15.000 Nachrichten über den Chat-Dienst WhatsApp verschicken. »Eine Mutter erzählte mir, dass sie einmal ihrer 15-jährigen Tochter als Strafe für eine Nacht ihr Smartphone weggenommen hätte. Als sie es ihr am nächsten Tag wiedergeben wollte, hat sie gesehen, dass über Nacht rund 500 Nachrichten per WhatsApp eingegangen waren«, so Wüsten.

Bewusstsein für Grundsätzliches fehlt

In seinem Präventionsunterricht versucht Lorenz Wüsten bei den Jugendlichen ein Bewusstsein für einige zentrale Fragen der Sicherheit bei der digitalen Kommunikation zu schaffen – im Fokus stehen dabei Themen wie Identitätsschutz im Netz oder

SCHUTZ VOR CYBERGROOMING

Cybergrooming bezeichnet die Kontaktaufnahme erwachsener Täter zu Kindern oder Jugendlichen mittels Internet zur Anbahnung sexueller Handlungen.

- **> Sprechen Sie mit Ihren Kindern über die Problematik und achten Sie darauf, dass Ihre Kinder in Chats und Sozialen Netzwerken keine persönlichen Angaben wie Adresse und Telefonnummer machen.**
- **> Helfen Sie Ihren Kindern bei den Einstellungen für die Privatsphäre in Sozialen Netzwerken, um private Informationen nur für Freunde sichtbar zu machen.**
- **> Sprechen Sie mit Ihren Kindern über den Begriff »Freund« in der realen und in der digitalen Welt.**
- **> Kinder und Jugendliche sollten verantwortungsvoll mit ihren Fotos und Videos umgehen und nicht alles posten.**
- **> Eltern und Pädagogen sind gefragt, sich mit dem Internet auseinanderzusetzen und sich gemeinsam mit den Kindern über mögliche Gefahren, aber auch den Nutzen des Internets auszutauschen.**

die Verbreitung von Foto- und Videomaterial. Am Beispiel von Personensuchmaschinen macht der Experte etwa deutlich, wie schnell man sehr detaillierte Informationen über eine Person im Internet finden kann – wenn die betreffende Person unvorsichtig mit privaten Daten umgeht. »Die Jugendlichen sind ernsthaft betroffen, wenn sie sehen, dass man mit nur wenigen Klicks ihr komplettes Leben einsehen kann. Von der amazon-Wunschliste über peinliche Fotos in Sozialen Netzwerken, Beiträge in Foren, private Informationen zu Hobbys und Freunden bis hin zu Privatadresse und Telefonnummer kann für völlig Fremde alles sichtbar sein«, so Wüsten. Auch die Geschwindigkeit, mit der sich Informationen und Bilder im Netz verbreiten, sei vielen Jugendlichen nicht bewusst. Beispiel Facebook: Viele Jugendliche gehen dort freizügig mit Informationen um, weil sie der Meinung sind »das sehen ja nur meine Freunde«. Nach der aktuellen »KIM-Studie« des medienpädagogischen Forschungsverbands Südwest haben 6- bis 13-Jährige bei Facebook im Schnitt 130 Freunde. »Ich rechne das dann ganz konkret vor: Denn die 130 Freunde haben auch wiederum 130 Freunde. Mit zwei Klicks ist man dann bei 17.000 Personen, die etwa ein Foto sehen und weiterverbreiten können – von Freunden kann da keine Rede mehr sein«, erklärt der Präventionsexperte.

Medienscouts führen Präventionsarbeit fort

Als wirksam hat sich die Ausbildung von so genannten »Medienscouts« gezeigt. Das sind ausgewählte Schülerinnen und Schüler, die in einem viertägigen Workshop alles Wichtige rund um die Sicherheit im Internet lernen und dies an die Klassenkameraden weitertragen. »Wir haben mit diesem Modell gute Erfahrungen gemacht, denn die Medienscouts scheinen bei ihren Mitschülern tatsächlich etwas bewirken zu können. Sie können eingreifen, wenn sie etwas Konkretes mitbekommen – etwa wenn ein Schüler gemobbt wird«, so Wüsten. >

PRÄVENTIONSTIPPS ZU SEXTING

Sexting beschreibt das Verschicken von E-Mails oder Messenger-Nachrichten mit erotischen Inhalten/Bildern, u. a. auch Nacktfotos von sich selbst, vor allem unter Jugendlichen.

- **> Klären Sie Ihre Kinder über die möglichen Gefahren von Sexting auf. Ist ein Foto einmal digital verschickt, lässt sich die Verbreitung weder kontrollieren noch stoppen.**
- **> Um sich davor zu schützen, dass derartige Bilder ungewollt an Dritte gelangen, ist es am einfachsten, solche Bilder erst gar nicht zu erstellen und auch nicht mit anderen zu teilen.**

Kaum ein Präventionssegment ist so anspruchsvoll wie der Bereich Cybercrime. Durch neue Techniken entstehen neue Problematiken und neue Tätigkeitsfelder. »Die Gesetze rund um das Thema sind aus dem letzten Jahrhundert – damals konnte man noch gar nicht absehen, welche Technologien heute zur Verfügung stehen. Und auch heute haben wir auf vieles noch keine Antwort, weil uns die technischen Entwicklungen vorauseilen«, meint der Experte.

Konkrete Beispiele zeigen Wirkung

Auch Horst Radtke von der Polizei Duisburg ist seit vielen Jahren in der Cybercrime-Prävention tätig und arbeitet hauptsächlich mit Eltern und Jugendlichen. Ein Thema, das ihn in dem Bereich immer wieder beschäftigt, sind Urheberrechtsverletzungen. Sein Rat für die Arbeit mit jungen Menschen: Möglichst konkrete Szenarien aufzeigen, um den Jugendlichen zu verdeutlichen, welche Konsequenzen gewisse Handlungsweisen haben können. »Jugendliche haben oft überhaupt kein Bewusstsein dafür, dass das Urheberrecht ein Menschenrecht ist. Dass ich, wenn ich zum Beispiel ein Bild kaufe, zwar das Recht habe, mir dieses Bild anzusehen, aber nicht, dieses Bild zu kopieren und an andere zu verteilen. Dass der Urheber dieses Bildes bestimmt, was damit passiert – und dass ich dieses Recht nicht verletzen darf«, so Radtke. Als konkretes Beispiel bringt der Präventionsexperte gerne das Beispiel von »Patrick«, der seit drei Jahren auf dem Schulhof gebrannte Musik und Filme an Mitschüler verkauft. Durch Zufall erfährt die Polizei davon. Es kommt zu einer Hausdurchsuchung, bei der sämtliche Rechner, auch die von den Eltern und der Schwester des 16-Jährigen für mehrere Wochen beschlagnahmt werden. Es kommt zu einer Anklage. Der Jugendrichter verurteilt Patrick zu 1.000 Euro Geldstrafe, während die geschädigte Plattenfirma von Patrick 10.000 Euro Schadenersatz fordert. Das Finanzamt fordert noch einmal 3.000 Euro, da Patrick mit den kopierten CDs und Filmen Handel betrieben hat und er somit einkommenssteuerpflichtig ist. »Ich rechne den Jugendlichen vor, dass in diesem konkreten Fall leicht 14.000 Euro zusammenkommen können, die zu zahlen sind – und zwar von Patrick selbst, nicht von seinen Eltern. Denn ab sieben Jahren ist man bedingt schadenersatzpflichtig – und ein Titel gilt immerhin 30 Jahre. Patrick kann also, wenn er mit 18 sein erstes Geld verdient, erst einmal anfangen, diese 14.000 Euro abzuzahlen.« Solche Beispiele wirkten bei den Jugendlichen – je konkreter man würde, desto besser, so der Experte.

Sexting: das Smartphone als Tatmittel

Auch beim Thema Sexting arbeitet Horst Radtke gerne mit konkreten Beispielfällen.Er führt den Jugendlichen vor Augen, wie schnell sie sich bei dem Thema strafbar machen können. »Wenn man Nacktbilder einer 13-Jährigen weiterleitet oder irgendwo hochlädt, kann das unter bestimmten Voraussetzungen unter »Verbreitung von Kinderpornografie« fallen. Auch wenn ich selbst noch minderjährig bin. Das ist den meisten überhaupt nicht bewusst«, so der Experte. Wirkung zeige auch der Hinweis, dass ein Smartphone in solch einem Fall ein Tatmittel ist. Und wenn der Staatsanwalt entscheidet, dass dieses Tatmittel vernichtet werden soll, dann kann es durchaus sein, dass das neue iPhone 6 in der Schrottpresse landet.

Viele der Jugendlichen sind außerdem der Meinung, dass, wenn sie Nacktfotos über den Dienst »Snapchat« versenden, die Bilder nach ein paar Sekunden automatisch gelöscht werden. Der Dienst wirbt zwar damit, Fakt ist aber: Es wird lediglich die Datei-Endung geändert, das Bild wird nicht endgültig gelöscht

PRÄVENTIONS-TIPP

SCHUTZ VOR CYBERMOBBING

Achten Sie darauf, dass Ihre Familienangehörigen (insbesondere Kinder) und Sie möglichst wenig private Daten im Internet preisgeben:

- **Geben Sie in Profilen von Sozialen Netzwerken niemals Ihre vollständige Adresse oder Telefonnummer an.**
- **Stellen Sie möglichst wenige Bilder oder Videos von sich selbst ins Profil.**
- **Sorgen Sie über die Sicherheitseinstellungen des Sozialen Netzwerks für einen privaten Bereich, den Sie auch nur für tatsächliche Freunde freigeben sollten.**
- **Sollten Sie selber Opfer von Cybermobbing sein, vertrauen Sie sich der Familie, Freunden oder anderen Vertrauenspersonen an.**
- **Sichern Sie Beweismaterial (in Form von Screenshots bei Chats, beleidigende E-Mails oder SMS).**
- **Erstatten Sie in schwerwiegenden Fällen Anzeige bei der Polizei.**
- **Bei Cybermobbing in Sozialen Netzwerken wenden Sie sich an den Betreiber der Seite, um ggf. das Profil des Mobbenden löschen oder sperren zu lassen.**
- **Betreuen Sie Ihre Kinder im Umgang mit dem Internet – achten Sie aber darauf, Raum für Privatsphäre zu lassen. Klären Sie Ihre Kinder über mögliche Folgen eines Datenmissbrauchs auf, seien Sie offen für Fragen, und helfen Sie, wenn es zu Problemen kommen sollte.**

In fünf Filmen des Landespräventionsrates wird ein konkreter Cybermobbing-Fall aus ganz unterschiedlichen Perspektiven dargestellt: www.sichere-netzwelten.de

und befindet sich immer noch auf dem Handy des Nutzers, der die Fotos somit immer noch weiterverbreiten kann. »Die Jugendlichen sind häufig sehr geschockt, wenn sie dieses erfahren – man kann nur hoffen, dass sie ihr Verhalten diesbezüglich in Zukunft überdenken.«

Datensicherheit bei Facebook

Der Bereich Datensicherheit, gerade in Sozialen Netzwerken, ist ein weiterer Bereich, der den Präventionsexperten stark beschäftigt. Denn so gut wie niemand schaut zum Beispiel in die Nutzungsbestimmungen von Facebook. Dabei steht dort ganz genau, was konkret mit allen Inhalten eines Nutzers passiert. Es heißt dort: »Deine Privatsphäre ist uns sehr wichtig. In unserer Datenrichtlinie machen wir wichtige Angaben dazu, wie du Facebook zum Teilen von Inhalten mit anderen verwenden kannst und wie wir deine Inhalte und Informationen sammeln und verwenden können.« Weiter heißt es: »Du gewährst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz zur Nutzung jedweder IP-Inhalte, die du auf bzw. im Zusammenhang mit Facebook postest (»IP-Lizenz«). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst, es sei denn, deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht.« »Ich mache den Schülerinnen und Schülern hier noch einmal ganz deutlich: »Egal, was ihr auf Facebook postet oder hochladet, ihr gebt Facebook das Recht, alles mit euren Daten zu machen und sogar an andere zu verkaufen – überlegt euch, was ihr dort hineinstellt«, so Radtke.

Der Experte betont, wie wichtig die polizeiliche Prävention im Bereich Cybercrime ist, denn die Botschaften werden von einem Polizeibeamten anders wahrgenommen als von Eltern oder >

Foto: Jochen Tack

»Jugendliche haben oft überhaupt kein Bewusstsein dafür, dass das Urheberrecht ein Menschenrecht ist.«

Horst Radtke,
Präventionsbeamter des PP Duisburg

Lehrern. Prävention sei Aufklärung und heiße, zu wissen, was man dürfe und was nicht. Wie man mit diesem Wissen hinterher umgehe, müsse jeder selbst entscheiden – dann aber auch die Konsequenzen tragen. »Es entsteht oft der Eindruck, ich hätte etwas gegen das Internet. Oder Facebook. Oder WhatsApp. Das habe ich nicht, ich nutze diese Dienste selbst auch. Man muss aber wissen, wie man sie nutzt – und die Vor- und Nachteile kennen«, so Horst Radtke.

Retouren-Überweisungen

Michael Paech von der Polizei Essen bereiten ganz andere Dinge Sorgen, denn er hat als Cybercrime-Ermittler hauptsächlich mit Organisierter Kriminalität im Bereich Cybercrime zu tun. Paech beschäftigt sich mit der Auswertung von Netzwerkverkehr und Asservaten sowie mit Serverüberwachungen. Dass Cyberkriminelle immer erfindungsreicher werden, bekommt auch er zu spüren. »Die Schadprogramme werden immer komplexer. So genannte Ransomware, also Schadsoftware, die den Rechner verschlüsselt und ein Lösegeld fordert, beschäftigt uns seit einiger Zeit besonders«, erklärt der Experte. Manche Varianten der Schadsoftware verschlüsseln aber nicht nur den Rechner und erpressen den Nutzer um 100 Euro, sondern laden noch weitere Schadsoftware nach. Ein Banking-Trojaner greift dann sämtliche Bankdaten, E-Mail-Adressen, Passwörter, aber auch FTP-Server-Log-ins, also Zugangsdaten zu fremden Webseiten ab, die auf dem Rechner zu finden sind. Der Trojaner ist außerdem auf so genannte Retouren-Überweisungen spezialisiert. Er ist so programmiert, dass er, sobald man sich auf der Webseite seiner Bank einloggt, die eingegebenen Daten abfängt und im Browser ein neues Fenster einblendet, mit der Nachricht, es habe eine Fehlbuchung auf das Konto gegeben, die man zurücküberweisen solle. Die Schadsoftware prüft dabei im Hintergrund den aktuellen Kontostand und das maximale Überweisungslimit – und bildet daraufhin eine passende Summe, die angeblich zu viel überwiesen wurde. Diese Summe wird dann tatsächlich auch im Kontoverlauf im Bereich »Guthaben« angezeigt. Der Nutzer überweist die angezeigte Summe – und das Geld landet bei den Betrügern. »Dieser Trojaner hat es hauptsächlich auf deutsche Bankdaten abgesehen. Insgesamt gehen wir von 30.000 bis 40.000 betroffenen Rechnern aus – die Schäden liegen im Millionenbereich«, so Paech. Und damit nicht genug: Die Schadsoftware befällt auch Smartphones und ist in der Lage, mTANs abzufangen. Anschließend wird zunächst das Kontolimit hochgesetzt und dann das Konto leergeräumt.

Organisierte Kriminalität oder Trojaner-Kits

Bei derartig komplexem Vorgehen und hohen Schadenssummen sind in der Regel Täter am Werk, die hoch spezialisiert und gut organisiert sind. »Man braucht für solche groß angelegten Angriffe jede Menge Server, eine häufig aktualisierte Schadsoftware, eine möglichst in vielen Sprachen und vor allem fehlerfreie getextete Phishing-Mail oder andere glaubhafte »Köder« sowie für jede Bank das passende Pop-up-Fenster mit Logo und Layout – das erfordert schon einiges an Manpower«, weiß Michael Paech. Die Ermittlungen in solchen Fällen sind arbeitsintensiv und aufwändig. Man braucht Geduld, die zum Teil aber auch belohnt wird. »Selbst die Profis machen Fehler, denn auch das sind nur Menschen. Wenn wir jemanden schnappen, dann liegt es häufig an menschlichem Versagen – nicht an technischem«, so der Experte. Neben der Organisierten Kriminalität gibt es jedoch auch Fälle,

»Jeder muss einen aktiven Beitrag leisten, um seine Daten, sein Geld und seine Privatsphäre zu schützen.«

Michael Paech,
Cybercrime-Ermittler des PP Essen


Foto: Jochen Tack

bei denen sich die Täter als Jugendliche oder Kinder entpuppten, die sich im Internet Trojaner-Kits, also fertige Baukästen für Schadsoftware, besorgt hatten, und das Ganze mal ausprobieren wollten. »Für diese Baukästen brauche ich kein großes Technikverständnis, ich kann mir die passende Schadsoftware einfach selbst zusammenstellen. Ich hatte schon 13-Jährige in der Vernehmung sitzen, die eigene Bot-Netze mit mehreren Tausend Geschädigten betrieben haben«, so Paech.

Schutz von Smartphones wird vernachlässigt

Ebenfalls Sorge bereitet dem Experten die zunehmende Verbreitung von Schadcode über Smartphones. Dazu trage vor allem auch das fehlende Bewusstsein der Nutzer bei. »Kaum jemand hat eine Antivirensoftware auf seinem Smartphone, dabei ist das Gerät genau wie ein Computer zu behandeln«, betont der Experte. Malware gelangt vor allem über E-Mails, Spiele-Seiten oder Apps auf die Smartphones. »Wenn etwa eine Taschenlampen-App Berechtigungen wie einen vollen Systemzugriff, E-Mail-Versand und Internetzugriff verlangt, sollte man stutzig werden«, so Paech. Ob das Smartphone mit Schadsoftware infiziert ist, merkt man als Nutzer häufig nicht. Ein Hinweis kann jedoch ein im Vergleich zur sonstigen Nutzung hoher Verbrauch an Datenvolumen sein.

»Jeder muss einen aktiven Beitrag leisten, um seine Daten, sein Geld und seine Privatsphäre zu schützen. Man muss sich bewusst werden: Jeder gekaperte Rechner, jeder gehackte Account und jede gestohlene E-Mail-Adresse bringt den Cyberkriminellen Geld. Da kann niemand sagen: »Das interessiert mich nicht«.« ///

Simone Wroblewski

PRÄVENTIONS-TIPP

SCHUTZ FÜR SMARTPHONES UND TABLETS

- **Sorgen Sie mit aktivierten Sperrcodes dafür, dass niemand ohne weiteres an die Informationen auf Ihrem Smartphone oder Tablet gelangen kann.**
- **Aktivieren Sie Netzwerkverbindungen (Bluetooth, WLAN) nur, wenn Sie sie auch benötigen.**
- **Auch auf Smartphone und Tablet sollte ein Virenschutzprogramm installiert sein.**
- **Halten Sie das Betriebssystem Ihres Smartphones und Tablets sowie alle installierten Apps auf dem neuesten Stand.**
- **Laden Sie Apps nur aus vertrauenswürdigen Quellen herunter. Informieren Sie sich über Apps im Internet.**
- **Achten Sie darauf, welche Funktionen oder Berechtigungen eine App besitzt bzw. bei der Installation anfordert. Braucht eine App wirklich alle geforderten Berechtigungen, damit sie funktioniert?**
- **Wenn Sie Ihr Smartphone oder Tablet verkaufen oder verschenken, sorgen Sie dafür, dass Ihre persönlichen Daten darauf richtig gelöscht werden. Es gibt spezielle Apps, die das Smartphone »wipen«, d. h. alle Daten löschen und mehrfach überschreiben.**

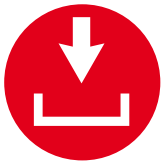
Mehr Infos zum sicheren Umgang mit Apps zeigt das Video »Smartphone Apps« des Landespräventionsrats NRW: www.sichere-netzwelten.de

Die wichtigsten Cybercrime-Phänomene

Cybercrime hat viele Gesichter. Aber was verbirgt sich hinter Begriffen wie »Cybergrooming«, »Ransomware« oder »Sexting«? Und was passiert bei einem Identitätsdiebstahl? Die Streife erklärt die wichtigsten Begriffe und Phänomene rund um Cybercrime.

CYBERCRIME

Cybercrime ist Kriminalität unter Nutzung von Informations- und Kommunikationstechnik. Delikte aus dem Bereich werden nach »Cybercrime im engeren Sinne« und »Cybercrime im weiteren Sinne« unterschieden. Cybercrime im engeren Sinne umfasst Straftaten, bei denen Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind. Cybercrime im weiteren Sinne bezeichnet Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung eingesetzt wird (Erlass des Ministerium für Inneres und Kommunales (MIK) vom 29. Februar 2012).



DRIVE-BY-DOWNLOAD

Beim Surfen auf einer manipulierten Webseite wird ein unzureichend geschützter Rechner mit Schadsoftware infiziert, ohne dass der Nutzer dazu aktiv etwas beitragen muss – wie etwa eine Datei anzuklicken.

DISTRIBUTED-DENIAL-OF-SERVICE-ANGRIFF (DDOS-ANGRIFF)

Bei einem Denial-of-Service-Angriff (DoS-Angriff) wird ein Server mit gezielten Anfragen regelrecht »bombardiert«. Er steht so für reguläre Anfragen nicht mehr zur Verfügung. Wird ein DoS-Angriff koordiniert und von einer größeren Anzahl anderer Systeme ausgeführt, so spricht man von einem DDoS-Angriff (Distributed Denial of Service-Angriff).

SOCIAL ENGINEERING

Social Engineering nutzt die »Schwachstelle Mensch« aus. Durch Täuschung werden die Opfer veranlasst, selbst Schadsoftware zu installieren oder den Tätern Zugang zu Systemen und Informationen zu gewähren.

RANSOMWARE

Unter Ransomware (engl. »ransom« = Lösegeld) versteht man Schadprogramme, die bei Betroffenen das gesamte Computersystem sperren oder die Nutzung des Computers sowie den Zugriff auf Daten nur teilweise ermöglichen. Diese Schadprogramme gelangen beispielsweise über präparierte E-Mail-Anhänge oder das Anklicken manipulierter Werbebanner auf Webseiten auf den Rechner. Ist der Computer infiziert, erscheint auf dem Bildschirm ein Pop-up-Fenster mit der Nachricht, dass der Rechner erst wieder freigegeben wird, wenn man eine bestimmte Geldsumme an die Cyberkriminellen zahlt. In der Regel wird der Nutzer dann aufgefordert, den geforderten Betrag über einen digitalen Bezahldienst wie etwa Paysafecard oder Ukash zu übermitteln. Im Anschluss erhält der Betroffene einen Freigabecode. Besonders perfide sind die Betrugsvarianten, bei denen die Betrüger vorspiegeln, sie arbeiteten für offizielle Stellen wie etwa das Bundeskriminalamt oder die Bundespolizei. Dabei wird dann zum Beispiel behauptet, dass der Rechner im Zusammenhang mit der Verbreitung kinderpornografischen Materials, bei terroristischen Aktionen, Urheberrechtsverletzungen oder anderen Straftaten genutzt worden sei – deshalb würde der Computer gesperrt und man müsse eine Strafe zahlen. »Die Täter nutzen zum Teil Schadsoftware, die nicht nur täglich, sondern zum Teil stündlich aktualisiert wird. Das macht es Antivirenprogrammen sehr schwer, den Schadcode zu erkennen«, erklärt Michael Paech vom PP Essen.

ERPRESSUNG

Sowohl Privatpersonen als auch Unternehmen können im Rahmen von Cybercrime von Kriminellen erpresst werden. Dazu dienen neben dem Einsatz von Ransomware auch DDoS-Attacken. Dabei werden Betreiber von Online-Geschäften oder gewerblichen Internetauftritten per E-Mail aufgefordert, einen vergleichsweise geringen Betrag von bis zu 2.500 Euro an die Täter zu zahlen. Erfolgt die Zahlung nicht bis zu einem bestimmten Zeitpunkt, wird der Internetauftritt oder der Online-Shop lahmgelegt. Dies kann innerhalb kurzer Zeit zu hohen Umsatzverlusten bei den Betreibern der Internetauftritte führen, so dass Geschädigte oft bereit sind, das vergleichsweise geringe »Schutzgeld« zu zahlen. Privatpersonen werden beispielsweise mit heimlich aufgenommenen Nacktaufnahmen erpresst – zum Beispiel von Kontakten in Chatforen mittels der integrierten Computerkamera. »Die Anzahl der Anzeigen in diesem Bereich sind sehr gering. Unternehmen befürchten einen Image-Schaden oder weitere Betriebsausfälle. Privatpersonen ist es häufig peinlich, sich an die Polizei zu wenden, wenn sie mit Nacktaufnahmen erpresst werden«, so Michael Paech vom PP Essen.

MAN-IN-THE-MIDDLE-ANGRIFF

Bei dieser Angriffsform sitzt der Angreifer zwischen zwei Kommunikationsendpunkten und kann den Datenverkehr manipulieren.

CYBERMOBBING

Unter Cybermobbing (auch Cyberbullying genannt) versteht man das Beleidigen, Bloßstellen, Bedrohen oder Belästigen einer Person mithilfe moderner Kommunikationsmittel wie Computer, Handy oder Smartphone über einen längeren Zeitraum. Das Phänomen kann insgesamt verschiedene Straftatbestände umfassen – wie etwa Beleidigung, üble Nachrede, Verleumdung, Verletzung der Vertraulichkeit des Wortes, Nachstellen, Nötigung, Erpressung oder die Verletzung des Rechtes am eigenen Bild. Die rechtliche Erfassung von Cybermobbing als Ganzes ist schwierig, da es sich um viele Einzeltaten handelt, die sehr unterschiedlich ausgeprägt sein können.
Unter Kindern und Jugendlichen ist Cybermobbing weit verbreitet. Kaum eine Schule kämpft nicht mit diesem Thema. »Cybermobbing beinhaltet viele Aspekte, die sich rechtlich gar nicht erfassen lassen und trotzdem große Auswirkungen auf die Opfer haben – etwa wenn sie ständig ausgegrenzt oder wie Luft behandelt werden«, weiß der Präventionsexperte Lorenz Wüsten vom PP Bonn.

IDENTITÄTSDIEBSTAHL

Dabei verschaffen sich Cyberkriminelle Zugang zu einem fremden Account und nutzen diesen für kriminelle Machenschaften – etwa, um Bekannte und Freunde des Opfers zu täuschen und über diese an Geld zu kommen. Account-Übernahmen finden aber auch im Rahmen von Cybermobbing statt, indem etwa der Account des Opfers in einem Sozialen Netzwerk geknackt wird. Im Anschluss nutzen die Täter diese Plattform, um das Opfer bloßzustellen oder lächerlich zu machen.

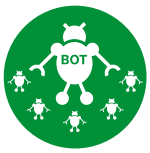
Ein Beispiel: Betrüger hacken den Facebook-Account eines Mitglieds. Im Anschluss versenden sie Nachrichten über diesen Account an seine Facebook-Freunde mit der Bitte, ihre Handynummer zu übermitteln. Geschieht dies, erhalten die Freunde bald eine SMS auf ihr Handy, die verschiedene Codes enthält. Diese sollen sie an den vermeintlichen »Freund« weiterleiten, denn die Codes seien aus Versehen bei ihnen gelandet. »Was die Getäuschten nicht wissen: Bei den Codes handelt es sich um TANs eines SMS-Bezahldienstes, der über die Handyrechnung abgerechnet wird. Während die Betrüger die weitergeleiteten TANs für Shopping-Trips nutzen, landen die Kosten dafür auf der nächsten Mobilfunkrechnung der Geschädigten«, erklärt Horst Radtke, Präventionsexperte vom PP Duisburg.

PHISHING

Der Begriff »Phishing« setzt sich aus den Begriffen »Password«, »harvesting« und »fishing«, zusammen; also Passwort, abernten und fischen. Man versteht darunter das unberechtigte »Abfischen« von Passwörtern und Zugangsdaten zu Bankkonten oder Online-Shops sowie von Kreditkartendaten. Um Zugangsdaten zu erlangen, schleusen die Täter Schadsoftware auf einen Rechner, der die Informationen abfängt, ohne dass der Nutzer es bemerkt. Diese Daten werden zum Beispiel durch »Man-in-the-middle«-Angriffe innerhalb von Transaktionsvorgängen so manipuliert, dass schließlich Geldbeträge unbemerkt auf Täterkonten umgeleitet werden können. Darüber hinaus nutzen Täter manipulierte Webseiten und gefälschte E-Mails, um Opfer zur Preisgabe ihrer persönlichen Daten zu bewegen. Als Reaktion auf die Verbesserung der technischen Sicherheitsstandards insbesondere beim Online-Banking setzen die Täter beim Phishing zunehmend auf Social Engineering.

TROJANER

Ein als harmlose Software getarntes Schadprogramm, das zum Beispiel eingesetzt wird, um Zugangsdaten auszuspähen.



BOT-NETZE

Der Begriff »Bot« leitet sich von dem Wort »robot« ab, also »Roboter«. Gemeint ist damit die Fernsteuerung eines Rechners durch Cyberkriminelle. Der Zusammenschluss von mehreren, meist vielen Tausend »Zombie-Rechnern«, die unter der Kontrolle von Internetbetrügern stehen, nennt man dementsprechend »Bot-Netz«. Damit ein Rechner Teil eines Bot-Netzes wird, muss er vorher mit Schadsoftware infiziert werden. Dies geschieht zum Beispiel über präparierte E-Mail-Anhänge oder Schadcode auf Webseiten, zu denen Links in E-Mails, Sozialen Netzwerken oder Messengern verbreitet werden. Dass sein Rechner an ein Bot-Netz angeschlossen wurde, merkt der Nutzer selbst meist gar nicht. Im Hintergrund nutzen die Cyberkriminellen seine Rechenkapazität jedoch dazu, um Spam-Mails zu versenden, Schadcode zu verbreiten oder Denial-of-Service-Angriffe durchzuführen. »Viele Menschen sind sich nicht bewusst, was es bedeutet, wenn der eigene Rechner Teil eines Bot-Netzes ist – »Ich merke davon ja nichts«, heißt es dann oft. Fakt ist aber: Wird mithilfe des Rechners eine Straftat begangen und taucht die IP-Adresse des Computers im Zuge von Ermittlungen auf, ist der Besitzer des Rechners erst einmal tatverdächtig«, erklärt Horst Radtke vom PP Duisburg.

SEXTING

»Sexting« setzt sich aus den Begriffen »Sex« und »texting« zusammen und meint das Verschicken von E-Mails oder Messenger-Nachrichten mit erotischen Inhalten, unter anderem auch Nacktfotos von sich selbst. Dieser Trend ist derzeit vor allem unter Jugendlichen und jungen Erwachsenen verbreitet. Der elektronische Versand von persönlichen Bildern mit erotischem Charakter birgt jedoch Risiken: Schnell können sie in Soziale Netzwerke gelangen oder allgemein im Internet verbreitet werden. Diese Bilder können dann unter anderem für Cybermobbing, aber auch für Erpressungen genutzt werden. Auch bei der Jobsuche kann dies zu Problemen führen, wenn zukünftige Arbeitgeber im Internet auf solche Fotos stoßen. Und einmal im Netz, lassen sich die Bilder nicht mehr löschen. »Eine 16-jährige Schülerin hat etwa Nacktbilder von sich gemacht und an ihren Freund geschickt. Dieser hat die Fotos dann an mindestens zehn Personen weitergeleitet, welche die Bilder daraufhin vermutlich auch weitergegeben haben. Die Verbreitung solcher Inhalte kann man weder steuern noch stoppen – dessen muss man sich bewusst sein«, betont Lorenz Wüsten vom PP Bonn.

CYBERGROOMING

Cybergrooming bezeichnet die Kontaktaufnahme von Erwachsenen zu Kindern und Jugendlichen über das Internet zur Anbahnung von sexuellen Handlungen. Dabei werden die Kinder häufig dazu aufgefordert, selbst sexuelle Handlungen an sich vorzunehmen oder es wird ihnen pornografisches Material präsentiert. Die Opfer bewerten solch ein Verhalten oftmals zunächst nicht als strafbare Handlung, denn für viele Kinder und Jugendliche ist die Annäherung mit sexuellen Motiven bereits selbstverständlicher Teil der Kommunikation im Internet. Aus diesem Grund erfahren häufig weder Eltern noch die Polizei von diesen Annäherungen, so dass von einem großen Dunkelfeld auszugehen ist.
Ein Beispiel: Ermittler der Zentralen Internetrecherche des LKA NRW identifizierten in einem Fall von Cybergrooming einen 32-jährigen Tatverdächtigen, der in Sozialen Netzwerken Chat-Kontakt zu Minderjährigen suchte. Er sendete ihnen Nachrichten mit sexualbezogenem Inhalt und versuchte, reale Treffen mit ihnen zu verabreden. Über die Notruffunktion im Chat gingen daraufhin 228 Notrufe bei dem Chat-Betreiber ein, die dem Tatverdächtigen zugeordnet werden konnten – insgesamt verwendete er in den Chats 37 Pseudonyme. Zu einem realen Treffen zwischen den Minderjährigen und dem Tatverdächtigen ist es nicht gekommen.

URHEBERRECHT

Das Urheberrecht schützt die ideellen und materiellen Interessen des Urhebers an seinem Geistesswerk. Der Begriff Urheberrecht umfasst die Summe aller Rechtsnormen, die das Verhältnis des Urhebers und seiner Rechtsnachfolger zu seinem Werk regeln.

VIRUS

Ein Virus ist ein Schadprogramm, das unberechtigt in Systeme eindringt und dort Schaden anrichtet, Daten ausspäht und sich häufig auch reproduziert. Ein Antivirenprogramm soll vor Schadprogrammen schützen und diese von bereits betroffenen Systemen entfernen.

/// Simone Wroblewski

INTERVIEW

Landeskriminaldirektor Dieter Schürmann im Gespräch »Wir brauchen digitales Denken für Ermittler und Einsatzkräfte«

Die Welt wird in Zukunft noch digitaler als sie es heute schon ist. Durch das »Internet der Dinge« könnte bald jedes Fahrzeug, aber auch jede Wohnung und jedes Haus samt Kühlschrank, Fernseher und Türschloss digital steuerbar sein. Das bietet einerseits mehr Komfort und viele ökologische sowie ökonomische Vorteile. Gleichzeitig muss man aber auch die Risiken dieser Entwicklungen sehen, denn auch Kriminelle nutzen diese Techniken für ihre Zwecke. Somit werden analoge Formen der Tatbegehung immer mehr zu digitalen – die von der Polizei aber auch als solche erkannt werden müssen. Wie die Polizei NRW mit diesen Veränderungen umgeht, erklärt Landeskriminaldirektor Dieter Schürmann im Gespräch mit der »Streife«.

Streife: Welches Konzept verfolgt die Polizei, um sich personell im Bereich Cybercrime gut aufzustellen?

Schürmann: Wir brauchen in der Fläche einen kaskadenartigen Aufbau von Grundkenntnissen und landeszentral eine hohe Spezialisierung. Das heißt: Wir müssen alle Ermittlungs- und Einsatzkräfte in die Lage versetzen, einfache IT-relevante Sachverhalte zu verstehen und in einer Anzeige aufzunehmen. Mit einer IP-Adresse muss so selbstverständlich umgegangen werden, wie früher mit einer Telefonnummer. Auf der mittleren Ebene, also zum Beispiel im Rahmen der generellen kriminalpolizeilichen oder verkehrspolizeilichen Ermittlungsführung, bedeutet dies, dass die Beamten und Beamtinnen lernen, digitale Zusammenhänge zu erkennen und die entsprechenden Daten zu sichern. Sie müssen erkennen, welche Gefahren im Alltag von manipulierten IT-Systemen ausgehen können, um hier erfolgreich zu ermitteln.

Die dritte Ebene besteht aus dem Spitzensegment – dort findet sich auch das Cybercrime-Kompetenzzentrum des Landeskriminalamts. Dort werden ganz besondere Anforderungen an die IT-Fachkunde der Beschäftigten gestellt. Und dies sowohl was die Ermittlungen als auch die Gefahrenabwehr angeht, etwa bei Erpressungen, Geiselnahmen oder Angriffen auf kritische Infrastrukturen. Hierbei kommt es auch auf externes Know-how an: Wir brauchen z. B. junge, dynamische Hochschulabsolventen aus dem IT-Bereich, die mit den aktuellen Trends bestens vertraut sind und als IT-Spezialisten ihr Wissen bei uns einbringen. Wir sind hier technisch und personell schon sehr gut aufgestellt, müssen unsere Kompetenzen aber noch weiter ausbauen.

Streife: Welche konkreten Anforderungen stellt dies an die Aus- und Fortbildung bei der Polizei in NRW?

Schürmann: Der Trend geht zunehmend weg von der allein spezialisierten »Fortbildung Cybercrime«, weil IT mittlerweile allen Delikten zu eigen ist und dabei immer eine tragende Rolle spielen kann. Das heißt für uns, dass es zukünftig bei jedem Aus- und Fortbildungsbereich und zu jedem Phänomen auch eine digitale Komponente geben muss. Wir benötigen digitales Denken für alle Ermittler und Einsatzkräfte, aber auch in der polizeilichen Präventionsarbeit. Es macht keinen Sinn, den Bereich Cybercrime isoliert zu betrachten, weil diese Tatbegehungsformen mittlerweile

Fotos (2): Jochen Tack

alle Deliktsfelder durchdringen. Zum Spektrum der Verkehrsunfallaufnahme und Verkehrssicherheitsarbeit muss unseren Beamten etwa vermittelt werden, dass Fahrzeuge längst rollende Computer sind, die digitale Spuren ebenso erzeugen wie in sich tragen. Man muss wissen, dass auf Fahrzeugbetriebssysteme unter Umständen online zugegriffen werden und man es dadurch verunglücken lassen kann. Medizinisches Gerät kann gehackt, sabotiert und im schlimmsten Fall funktionsunfähig gemacht werden. So drohen sogar digital verübte Anschläge und Tötungsdelikte. Solche Tatbegehungsformen und Szenarien müssen unsere Ermittler aber erst einmal erkennen können, um sich dann zu erschließen, wie das technisch überhaupt möglich war. Auch hierzu ist die kreative Dimension des digitalen kriminalistischen Denkens gefordert. Und in der Präventionsarbeit geht es eben längst nicht mehr nur darum zu sagen: Bauen Sie einbruchhemmende Türen und Fenster ein, sondern: Sichern Sie Ihre Smart-Home-Steuerung gegen Cyberangriffe von außen. Das professionelle digitale Know-how der Polizei muss in allen ihren Aufgabenbereichen anforderungsgerecht vorhanden sein.

Streife: Wie kann und muss sich denn jeder Beamte selbst einbringen?

Schürmann: Digitales Bewusstsein geht im Prinzip jeden an. Jede Kollegin und jeder Kollege muss dies den Kernkompetenzen und der Professionalität der Polizei und der eigenen Aufgabe zuordnen. Mit jeder neuen technischen Anwendung entstehen neue Herausforderungen – aber auch neue Chancen, die die Polizei für ihre Arbeit nutzen kann. Gute Beispiele bieten hierfür die so genannten Sozialen Medien. Diese Entwicklung ist ein dynamischer Prozess, der immer schneller fortschreitet. Man kann nicht sagen: »Jetzt habe ich eine Fortbildung gemacht, jetzt bin ich fertig.« Man wird mit dem Thema niemals fertig sein. Cybercrime erfordert die große Bereitschaft, sich damit konsequent und fortlaufend auseinanderzusetzen. Das gilt für jeden: jüngere wie ältere, IT-erfahrene und IT-unerfahrene Kräfte. Die Polizei in NRW ist auf einem guten Weg, aber jeder muss sich auch selbst voranbringen. Wir dürfen nicht statisch bleiben, während die Welt sich weiterentwickelt. ///

Das Interview führte Simone Wroblewski

LANDESKRIMINALAMT NRW

Das Cybercrime-Kompetenzzentrum
Die zentralen Aufgabenbereiche

Das Landeskriminalamt Nordrhein-Westfalen mit Sitz in Düsseldorf ist die Landesoberbehörde für Kriminalitätsangelegenheiten und beschäftigt 1.150 Mitarbeiter. Seit 2011 ist das Cybercrime-Kompetenzzentrum die zentrale Ansprechstelle in allen Fragen der Cybercrime.

Zentrales Informations- und Servicezentrum (ZISC)

Die Beschäftigten des Zentralen Informations- und Servicezentrum Cybercrime (ZISC) beraten andere Behörden des Landes und des Bundes bei der Einsatzbewältigung und bei der Ermittlungsführung in Fällen herausragender Cybercrime. Hier ist auch die Zentrale Ansprechstelle Cybercrime (ZAC) mit dem Single Point of Contact (SPOC) angesiedelt, die rund um die Uhr an sieben Tagen die Woche erreichbar sind (SPOC-Statistik siehe Info-Kasten). Egal ob staatliche Behörden, Institutionen und Verbände aus Forschung und Lehre oder die Wirtschaft – an dieser zentralen Stelle erhalten sie fachkompetente Hilfe. »Im Fall der Fälle« werden hier alle wichtigen Sofortmaßnahmen initiiert und koordiniert.

Auswertung und Analyse Cybercrime

Tatzusammenhänge und neue Modi Operandi identifiziert die Auswerte- und Analysestelle Cybercrime. Sie bündelt die relevanten Informationen und leitet diese an die zuständigen Stellen der Kreispolizeibehörden, weiterer Behörden auf Landesebene sowie der anderen Landeskriminalämter und des Bundeskriminalamtes weiter. Basierend auf den eingehenden Informationen erstellen die Beschäftigten Analysen, Auswerteberichte, Lagebilder und Statistiken.

Prävention

Ziel der Arbeit im Bereich Prävention Cybercrime ist es, das Gefahrenbewusstsein (Awareness) zu steigern und wirkungsvolle Verhaltensweisen zur Gefahrenminimierung zu vermitteln. So sollen die Risiken, Opfer von Straftaten zu werden, gesenkt und Schäden verhindert werden. Im Cybercrime-Kompetenzzentrum werden landeseinheitliche Präventionskonzepte für die Kreispolizeibehörden erstellt. Im Rahmen von Messeauftritten und Vorträgen sowie mit Beiträgen im Intranet und Internet informieren die Mitarbeiterinnen und Mitarbeiter über konkrete Themen der Prävention im Bereich Cybercrime. Darüber hinaus ist das LKA NRW Mitglied im Landespräventionsrat NRW und koordiniert die Erstellung der Präventionsfilmreihe »Sichere Netzwelten«.

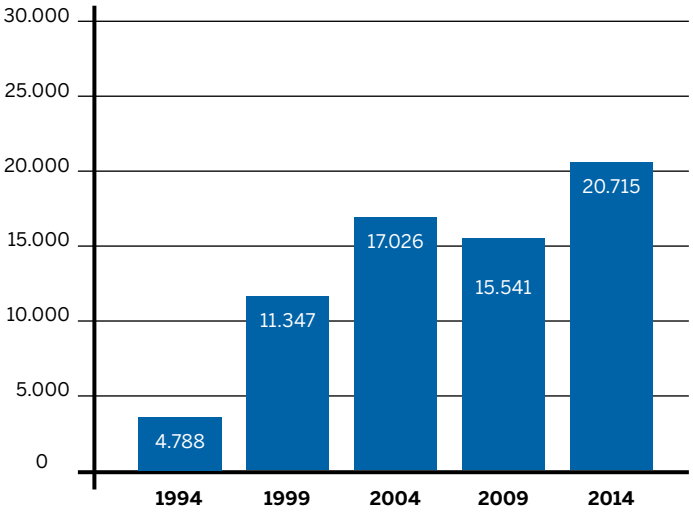
Zentrale Auswertungs- und Sammelstelle Kinderpornografie (ZAST)

In der ZAST werden gewaltverherrlichende, pornografische und jugendgefährdende Bild- und Videomaterialien ausgewertet. Bei den meisten Medien, die vorwiegend in digitaler Form vorliegen, handelt es sich um Kinderpornografie. Ziel der Auswertung ist es, Tatbeteiligte und Opfer des sexuellen Missbrauchs zu identifizieren, zum Beispiel durch Bestimmung der Tatzeit und des Tatortes. Die Zentralstelle koordiniert landesweit deliktspezifische Fahndungsmaßnahmen, deckt neue Tatbegehungsweisen auf und unterstützt die Kreispolizeibehörden bei ihren Ermittlungen.

Foto: Jochen Tack

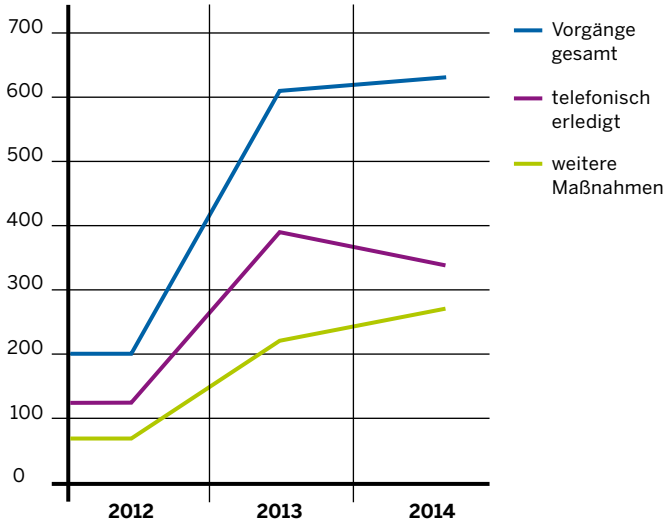
Die Experten des Cybercrime-Kompetenzzentrums bei ihrer Ermittlungsarbeit

Entwicklung der Fallzahlen im Bereich Cybercrime in NRW



Quelle: LKA NRW Lagebild Cybercrime

Vorgänge im Single Point of Contact (SPoC) 2012 – 2014



Quelle: Cybercrime-Kompetenzzentrum

Zentrale Internetrecherche (ZIR)

Die ZIR geht gezielt im Internet auf Streife, um Straftaten aufzudecken, Gefahren mit Bezug zum Internet abzuwehren und neue Phänomene zu entdecken und zu analysieren. Ein Ermittlungsschwerpunkt sind die Sozialen Netzwerke. Um Straftäter und Gefährder im Internet zu identifizieren, entwickelt sie immer wieder neue Methoden, die bedarfsweise von anderen Polizeidienststellen genutzt werden können. Darüber hinaus berät und unterstützt die ZIR Polizei-, Verwaltungs- und Justizbehörden, z. B. bei der Identifizierung von Tatverdächtigen, die versuchen, die Anonymität des Internets für ihre Straftaten zu nutzen.

Ermittlungskommissionen

Drei ständige Ermittlungskommissionen bearbeiten zum Teil jeweils mehrere Verfahren von herausragender Bedeutung gleichzeitig. Die meisten Verfahren weisen dabei komplexe technische Sachverhalte wie Kryptierungen und Anonymisierungen, neue Modi Operandi oder auch starke internationale Bezüge auf. Oft ist dabei die Zusammenarbeit mit ausländischen Ermittlungsbehörden erforderlich. In konkreten Einzelfällen entwickeln die Beschäftigten auch neue Ermittlungsmethoden und -werkzeuge.

Telekommunikationsüberwachung (TKÜ)

In Ermittlungsverfahren und bei Gefahrenlagen ist die Sicherung von Telekommunikationsdaten von hoher Bedeutung. Die TKÜ-Dienststelle des LKA NRW setzt alle Anträge der Polizeibehörden zur Sicherung von Inhaltsdaten (z. B. Telekommunikation der Tatverdächtigen) oder Verkehrsdaten (z. B. Standortfeststellungen zum Auffinden vermisster Personen) um. Ihre Mitarbeiterinnen und Mitarbeiter stehen bei technischen, taktischen und rechtlichen Fragestellungen der TKÜ rund um die Uhr als Ansprechpartner für alle Polizeibehörden in Nordrhein-Westfalen zur Verfügung.

Landeszentrale Ermittlungsunterstützung, Computerforensik

Egal ob Computerfestplatten oder Speicherbausteine aus Handys oder Navigationsgeräten – die Polizeibeamten und Ingenieure der IT-Forensik lesen die gespeicherten Daten aus elektronischen Geräten aus. Dabei suchen sie immer wieder nach neuen Wegen und Methoden, um auch bei kniffligen Fällen noch an deren Inhalte zu gelangen. Die gewonnenen Daten bereiten die Beschäftigten dann so auf, dass sie von den Ermittlern für ihre Verfahren weiter ausgewertet werden können. ///

Katerina Breuer

ERREICHBARKEITEN DES SPOC:

Landeskriminalamt NRW
Cybercrime-Kompetenzzentrum
Zentrale Ansprechstelle Cybercrime/Single Point of Contact
Telefon: +49 211 939-4040
Telefax: +49 211 939-194040
Mail: cybercrime.lka@polizei.nrw.de

CYBERCRIME-KOMPETENZZENTRUM

Wer steckt dahinter? Die Experten des Cybercrime-Kompetenzzentrums

»Bisher ist es uns immer gelungen, die Täter zu ermitteln. Das motiviert mich immer wieder aufs Neue. Da das Internet global ist und sich ständig ändert, gibt es immer wieder neue Begehungsweisen und zahlreiche internationale Bezüge. Die ständig komplexer werdenden Verfahren mit den vorhandenen Mitarbeitern zu bearbeiten – das ist immer wieder eine Herausforderung.«

MARKUS STEFFAN

ist 46 Jahre alt und leitet Ermittlungskommissionen im Dezernat 42. Er arbeitet bereits seit 2005 im Bereich Cybercrime. Seit 2012 ist er EK-Leiter im Cybercrime-Kompetenzzentrum. Hier werden Verfahren mit herausragender Bedeutung bearbeitet. Vor seinem Einstieg bei der Polizei Nordrhein-Westfalen hat er Wirtschaftsinformatik studiert.

»Die Arbeit im Cybercrime-Kompetenzzentrum ist ständig im Wandel – wie das Internet. Dadurch gibt es viele Möglichkeiten, eigene Ideen einzubringen, etwa bei der Planung von Veranstaltungen oder beim Entwerfen von Präventionsmaterialien. Ich arbeite mit vielen Kollegen aus unterschiedlichen Dienststellen zusammen, aber auch mit externen Kooperationspartnern – das ist sehr abwechslungsreich.«

NADJA KWASNY

ist 39 Jahre alt und arbeitet seit 2012 im Dezernat 41 im Bereich Prävention und Öffentlichkeitsarbeit. Sie bereitet Messen vor, begleitet Filmprojekte und schreibt Fachbeiträge für das Internet, Intrapol oder auch Pressemitteilungen. Vor ihrer Arbeit als Kriminalkommissarin hat sie Medienpädagogik studiert und in den Redaktionen von RTL und VOX gearbeitet.

»Gehören die Taten zusammen oder tritt hier etwa ein neuer Modus Operandi in Erscheinung? Das sind die Fragen, die ich im Hinterkopf habe, wenn ich die eingehenden Meldungen auswerte und weitersteuere. Die Kriminalitätslage zu überblicken und zum Beispiel Kolleginnen und Kollegen zusammenzubringen, die dann erfolgreich gemeinsam ermitteln – das macht die Arbeit spannend.«

MARIO LORENZ

ist 31 Jahre alt und seit 2012 im Dezernat 41 im Bereich Auswertung und Analyse. Hier laufen die Informationen zusammen, werden gebündelt und weitergeleitet. Mario Lorenz hat seine polizeiliche Laufbahn noch im mittleren Dienst begonnen und seinen Weg nach dem Wach- und Wechseldienst, der Hundertschaft und dem Aufstiegsstudium zum Cybercrime-Kompetenzzentrum gefunden.

Fotos (8): JJochen Tack

»Ich bin besonders stolz darauf, dass mit meiner Unterstützung jetzt auch fest verbaute Navigationssysteme aus Kraftfahrzeugen im Cybercrime-Kompetenzzentrum analysiert werden. Jedes Gerät bedeutet eine neue Herausforderung und viel Handarbeit und das macht es so spannend. Eine derartige Tätigkeit gibt es im Zusammenhang mit der Strafverfolgung nirgendwo sonst in NRW.«

CHRISTOPHER BELLINGHOFEN

ist 30 Jahre alt und seit 2012 bei der IuK-Ermittlungsunterstützung im Dezernat 43. Sein Schwerpunkt ist die forensische Sicherung und Untersuchung von tragbaren und fest verbauten Systemen zur Erfassung von Positionsdaten. Großteils handelt es sich dabei um Navigationsgeräte. Christopher Bellinghofen hat einen Bachelor of Science in Angewandter Informatik.

»Sind diese Bilder und Videos schon bekannt oder neu? Ist darauf vielleicht sogar ein aktueller Kindesmissbrauch zu sehen? Das sind hier die zentralen Fragen. Ich höre oft: »Oh Gott, da könnte ich nicht arbeiten.« Ich nehme die Arbeit jedoch nicht mit nach Hause. Es spornt mich an, daran teilzuhaben, dass ein aktueller Missbrauch beendet wird.«

PATRIC SCHÖNENBERG
ist 44 Jahre alt und arbeitet seit 2012 im Dezernat 43 bei der Zentralen Auswertungs- und Sammelstelle Kinderpornografie (ZAST). Neben Kinderpornografie landen auch andere jugendgefährdende Medien wie zum Beispiel Gewaltvideos auf seinem Schreibtisch. Zuvor war er lange Jahre bei der Beweissicherung der Hundertschaft und als Lehrender beim Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten (LAFP) NRW tätig.

»Aus einem Anruf kann sich ad hoc eine große Ermittlungskommission ergeben. Es kann aber auch sein, dass man alle Fragen direkt schon am Telefon beantworten kann. Daher muss man in dem Bereich ein Allrounder sein, der sich in allen Cybercrime-Bereichen auskennt und weiß, wann er weitere Experten hinzuziehen sollte.«

WOLFGANG HOLZAPFEL
ist 37 Jahre alt und beschäftigt sich seit 2008 mit der Cybercrime-Bekämpfung. Seit Mitte 2012 arbeitet er beim Zentralen Informations- und Servicezentrum Cybercrime (ZISC) im Dezernat 41, bei dem auch die Zentrale Ansprechstelle Cybercrime (ZAC) angesiedelt ist. Hier laufen Anfragen aus Wirtschaft, Behörden und der Politik zusammen. Vor seiner Arbeit bei der Polizei hat er Berufsausbildungen zum Elektroniker und IT-Systemkaufmann gemacht.

»Wir fangen da an, wo die Kollegen im Land aufhören müssen. Zu uns kommen nur die kniffligen Fälle. Da muss man kreative Lösungen finden und häufig auch im Team agieren. Seit Ende vorletzten Jahres haben wir eine Fräse, mit der wir komplexe Schaltungen und Adapter für Speicherchips realisieren können. Dadurch können wir noch mehr Datenträger als bisher auslesen.«

NORBERT PAESCHEL
ist 47 Jahre alt und arbeitet seit 2012 im Dezernat 43 bei der Computerforensik. Seine Stärke sind Lösungen zur Datensicherung an Mobiltelefonen, bei denen eigene Schaltungen hergestellt werden müssen. Grund dafür ist seine Vorbildung: Bevor er Polizeivollzugsbeamter geworden ist, hat er eine Ausbildung zum Werkzeugmacher absolviert und vier Jahre in seinem Beruf gearbeitet.

»Wir schauen da genau hin, wo erfahrungsgemäß etwas passiert. Ich finde es spannend, die Leute aus ihrer Anonymität zu ziehen. Viele Straftäter verlieren den Bezug zu ihrem Handeln, weil sie über einen Nickname nicht unmittelbar identifizierbar sind. Das führt dazu, dass gerade junge Leute das Gefühl dafür verlieren, was für einen Schaden sie anrichten können. Ihnen das vor Augen zu führen, motiviert mich.«

TIM SANDER
ist 30 Jahre alt und seit 2013 bei der Zentralen Internetrecherche (ZIR) im Dezernat 42. Er geht gezielt im Internet auf Streife und sucht dabei vor allem nach Kinderpornografie sowie Arzneimittel- und Betäubungsmittelkriminalität. Tim Sander hat neben seiner Polizeiausbildung einen Bachelor in Bioinformatik und Genomforschung und einen Master in Molekularer Zellbiologie.

INTERVIEW

Das Erfolgsmodell Cybercrime-Kompetenzzentrum

Der Direktor des Landeskriminalamtes Nordrhein-Westfalen im Gespräch

Fotos (2): Jochen Tack

Uwe Jacob spricht über die Zukunft des Cybercrime-Kompetenzzentrums und die Vorteile, die es für das ganze Land bietet.

Streife: Was für eine Bilanz ziehen Sie nach nahezu vier Jahren Cybercrime-Kompetenzzentrum beim Landeskriminalamt Nordrhein-Westfalen?

Jacob: Ich ziehe eine durchweg positive Bilanz. Die Einrichtung des Cybercrime-Kompetenzzentrums war für das Land Nordrhein-Westfalen ein großer Schritt, da nicht nur Kräfte gebündelt, sondern auch neue Kräfte eingestellt wurden. Diese Bündelung wurde vielfach in Deutschland, aber auch in Europa etwa bei Europol, kopiert. Das zeigt, dass wir mit unserer Einschätzung richtig lagen, dass es einer Spitzenorganisation bedarf, die herausragende Verfahren bearbeitet, neue Methoden und Techniken entwickelt und die Kreispolizeibehörden unterstützt. Nicht zuletzt konnten wir durch eine zentrale Rufnummer, die 24 Stunden am Tag, sieben Tage die Woche erreichbar ist, das Vertrauen der Behörden und Unternehmen in die Polizei erhöhen und die Anzeigenbereitschaft steigern. Während 2012 dort rund 200 Anrufe eingingen, wurde die Hotline 2014 schon 612 Mal genutzt. Das heißt aber nicht, dass jetzt alles zentral bearbeitet wird. Wir brauchen die Kompetenzen vor Ort in den Kriminalkommissariaten und im Wachdienst. Es ist wichtig, dass wir nicht stehen bleiben, sondern weitere Schritte ins Auge fassen.

Streife: Worin liegt die Stärke eines solchen Kompetenzzentrums?

Jacob: Wenn Experten aus verschiedenen Fachgebieten sich alle zusammen einbringen, können Synergien genutzt werden und es kommt einfach ein Mehr heraus. Dabei hat sich das Zusammenwirken von Fachkriminalisten und IT-Ingenieuren bewährt. Es wurden bereits neue Wege und Techniken entwickelt, mit denen nun auch die Kreispolizeibehörden im Land arbeiten. Drei feste Ermittlungskommissionen bearbeiten Fälle von besonderer Komplexität oder mit internationalen Bezügen. So konnte etwa mit Informationen aus dem Cybercrime-Kompetenzzentrum, die im Zusammenhang mit einem Fall von Kinderpornografie ermittelt wurden, ein laufender Missbrauchsfall in den USA beendet werden. Das FBI konnte einen Jungen befreien, der jahrelang in einem Käfig gehalten worden war und zum Missbrauch angeboten wurde.

Streife: Inwiefern profitieren auch die Kreispolizeibehörden im Land von der gebündelten Expertise?

Jacob: Wir sind in puncto Cybercrime der zentrale Ansprechpartner im Land – auch für die Kreispolizeibehörden und das rund um die Uhr. Durch zentrale Kooperationen halten wir den Kontakt zu Forschung, Lehre und Wirtschaft und geben die gewonnenen Erkenntnisse weiter. Sei es in Dienstbesprechungen oder in direkten Kontakten. Wir konnten den Behörden auch schon neue technische Ermittlungstools und Ermittlungsmaßnahmen zur Verfügung stellen. Nicht zuletzt ist das Kompetenzzentrum prädestiniert dafür, die Cyberkriminalisten von morgen für das gesamte Land zu qualifizieren. Wir möchten perspektivisch noch stärker mit den §-4-Behörden zusammenarbeiten und ein Wissensnetzwerk Cybercrime schaffen.

Streife: Was sind die drei größten Herausforderungen in Bezug auf Cybercrime für das Kompetenzzentrum?

Jacob: Eine große Herausforderung ist sicherlich Big Data. Mittlerweile hat jeder Privatmann elektronische Daten, mit denen man ganze Bibliotheken füllen könnte. So analysierten die Ermittlungskommissionen allein 2013 circa 170 Terabyte Daten, die bei Straftätern sichergestellt worden waren. 2014 waren es bereits 350 Terabyte in einem einzigen Ermittlungsverfahren. Nur zur Verdeutlichung: Ein Terabyte besteht aus einer eins mit zwölf Nullen. Solche Probleme kann man nicht mehr nur mit mehr Personal lösen. Stattdessen haben wir gemeinsam mit unseren Partnern in der Wirtschaft angefangen, neue Werkzeuge zu entwickeln, mit denen diese unstrukturierten Massendaten automatisiert ausgewertet werden können. Die ersten Ergebnisse des Versuchs einer semantischen Analyse

waren vielversprechend. Eine weitere Entwicklung, die das gute Recht eines jeden Bürgers ist, ist die Zunahme der Anonymisierung und Kryptierung im Internet. Bei Ermittlungen stellt uns dieser Trend vor immer neue Herausforderungen. Die Cyberkriminellen werden auch immer internationaler. Während deutsche Hacker früher meist deutsche Server angriffen, nehmen mittlerweile die europaweiten Angriffe zu und insbesondere organisierte Tätergruppen agieren immer mehr international. Dadurch spielt die Rechtshilfe in unseren Verfahren häufig eine große Rolle.

Streife: Wie sieht die Zukunft des Cybercrime-Kompetenzzentrums aus?

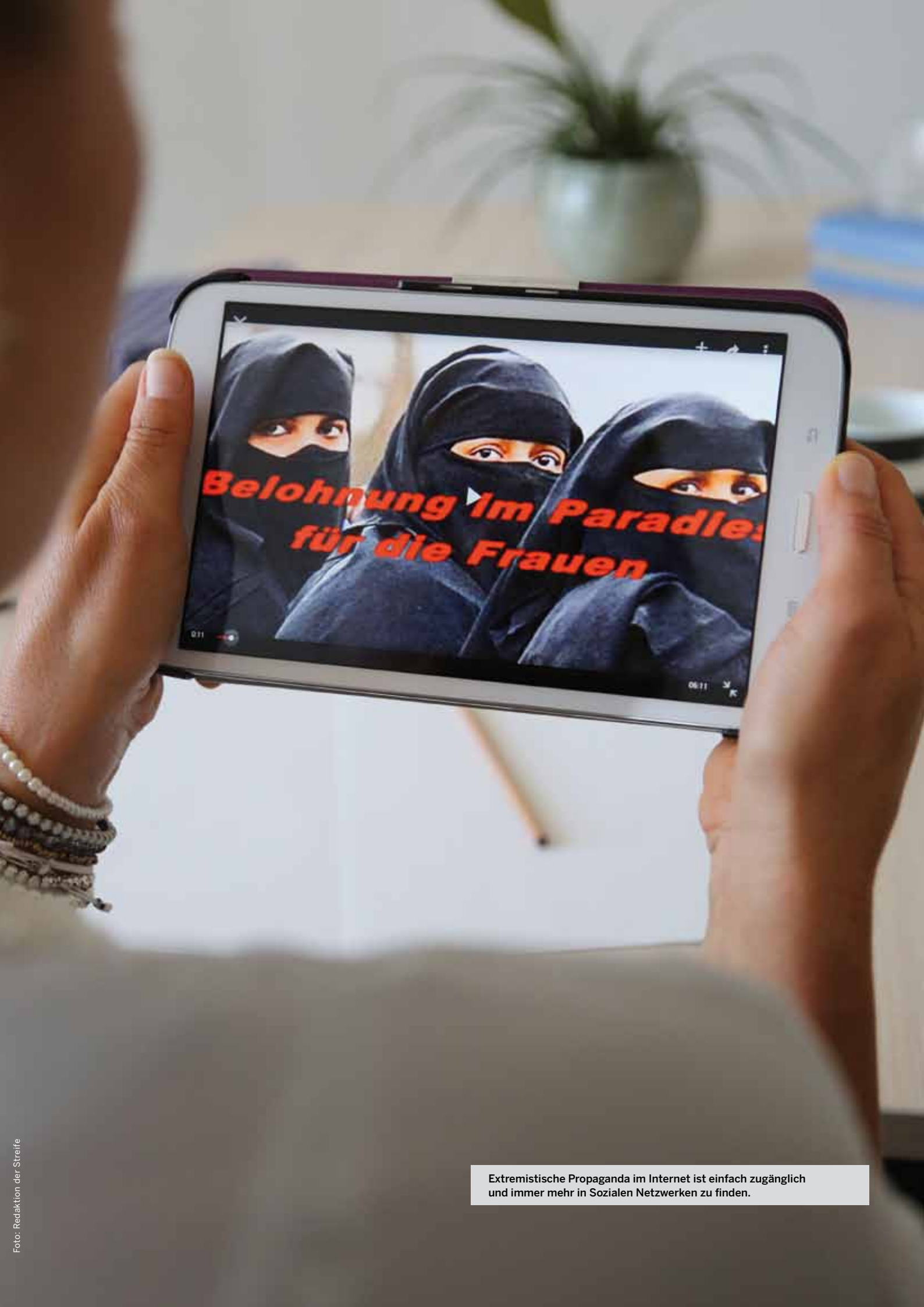
Jacob: Die Kolleginnen und Kollegen werden sich nicht über »Arbeitslosigkeit« beschweren können. Viele reale Straftaten verlagern sich ins Netz und ich denke, dass dieser Trend noch stärker zunehmen wird. Für einen erfolgreichen Kampf gegen Cybercrime werden wir auch zukünftig situativ angepasste Personalverstärkungen und eine stets aktuelle technische Ausstattung benötigen. Diese Prognose gilt im Übrigen nicht nur für das Cybercrime-Kompetenzzentrum, sondern auch für die Behörden im Land, die für eine erfolgreiche Bekämpfung der Cybercrime ein entscheidender Faktor sind.

Im Landeskriminalamt werden wir weiterhin effizientere Ermittlungsprozesse und neue Technologien entwickeln müssen. Und wir werden auch in Zukunft eng mit unseren Partnern in der Wirtschaft, Forschung und Lehre zusammenarbeiten müssen, denn nur wenn man Wissen bündelt, kann man innovative Ergebnisse erbringen. Die Entwicklungen in diesem Bereich sind sehr schnell. Das ganze Landeskriminalamt muss sich immer wieder in seiner Organisation an neue Gegebenheiten anpassen. Das wird gerade im Cybercrime-Kompetenzzentrum besonders deutlich. Aber bei all diesen organisatorischen Veränderungen müssen wir aufpassen, dass wir die Mitarbeiterinnen und Mitarbeiter in diesem ständigen Prozess mitnehmen.

Streife: Was würden Sie sich bei der Bekämpfung von Cybercrime für die Zukunft wünschen?

Jacob: Die Polizei ist zum Schutz der Bürger da und wir benötigen für den Schutz der Bürger die richtigen Instrumente und Ressourcen. Ich wünsche mir, dass mit Hilfe von Präventionsmaßnahmen das Bewusstsein in der Bevölkerung für den richtigen Umgang mit dem Medium steigt und sich die rechtlichen Entwicklungen an die tatsächlichen Gegebenheiten anpassen – Stichworte sind hier unter anderem: Novellierung der internationalen Rechtshilfe, Anpassen des formellen und materiellen Strafrechts sowie Schaffung einer nach den Vorgaben des Bundesverfassungsgerichts rechtsstaatlichen Regelung für die Vorratsdatenspeicherung. Die wichtigste »Ressource« ist jedoch in jedem Fall qualifiziertes und engagiertes Fachpersonal. ///

Das Interview führte Katerina Breuer



Extremistische Propaganda im Internet ist einfach zugänglich und immer mehr in Sozialen Netzwerken zu finden.

Foto: Redaktion der Streife

EXTREMISMUS

Cybercrime und politisch motivierte Kriminalität Islamistischer Terrorismus, Rechts- und Linksradikalismus im Netz

Auch im Bereich politisch motivierter Kriminalität spielt das Internet eine große Rolle: Ob Hackerangriffe, Aufrufe im Rahmen von islamistischer Propaganda, sich dem bewaffneten Kampf in Syrien oder dem Irak anzuschließen oder rechtsextremistische Hetze – die verschiedenen Gruppen nutzen das Internet gezielt für ihre Zwecke.

Der „Jihad im Internet“ ist mittlerweile ein weit verbreitetes Phänomen. Das Internet und insbesondere soziale Netzwerke werden zur Verbreitung salafistischer Propaganda intensiv genutzt. Kontaktanbahnungen sowie Anwerbungsversuche für extremistische und terroristische Netzwerke finden mittlerweile nicht mehr nur im „realen Leben“ statt, sondern haben häufig eine virtuelle Komponente. Als große Gefahr ist zudem islamistisch-motiviertes Hacking anzusehen. Die Anfälligkeit der digitalen Infrastruktur in Deutschland ist in den letzten Monaten sehr deutlich geworden. Der Zusammenbruch eines der Netze im deutschen Bundestag zeigt, dass Hackergruppen und ausländische Nachrichtendienste bereits in den „Cyber-Krieg“ eingestiegen sind. Möglichkeiten dieser Kriegsführung stehen auch salafistisch-terroristisch orientierten Gruppierungen grundsätzlich offen. Denn trotz ihrer rückwärtsgewandten Ideologie sind Salafisten heute technikaffin und nutzen konsequent die Möglichkeiten moderner Medien.

Auch in NRW wurden im Jahr 2015 Hackerangriffe auf Internetpräsenzen von Firmen und Vereinen festgestellt. Die Internetseiten wurden unbrauchbar gemacht und ihr Inhalt durch islamistische Logos ersetzt. >

Video-Naschid des Jihadisten Silvio K., ehemals Millatu-Ibrahim

Der islamistische Terrorismus nutzt das Internet seit vielen Jahren für eigene Zwecke. So versuchte Al-Qaida erstmals im Vorfeld der Bundestagswahl 2009 durch im Internet veröffentlichte Drohvideos in deutscher Sprache Einfluss auf das Wählerverhalten in Deutschland zu nehmen. Sie stammten von einem deutsch-marokkanischen Sprecher, der aus Nordrhein-Westfalen in das afghanisch-pakistanische Grenzgebiet ausgereist war. Auch vor der Bundestagswahl 2013 erfolgten Drohungen aus islamistischen Kreisen über Videos im Internet.

Seitdem ist im Internet islamistische Propaganda zunehmend auch in deutscher Sprache festzustellen. In professionellen Videobotschaften erfolgen Aufrufe an in Deutschland lebende Muslime, in Krisengebiete wie Syrien oder Irak auszureisen und sich dort dem bewaffneten Kampf anzuschließen. Diese Appelle werden häufig in Form von Anaschid (Plural von »Naschid«, arabisch für Propagandalieder mit islamisch-religiösem Inhalt) vorgetragen. Junge Frauen werden aufgefordert, sich dort mit Kämpfern der Terrororganisation verheiraten zu lassen. Zunehmend enthalten diese Videobotschaften auch direkte Drohungen gegen Deutschland. Dabei werden auch vermeintliche und tatsächliche islamkritische Tendenzen, z. B. aus dem rechten Spektrum, als Begründung angeführt.

Intensive Beobachtung nötig

Die islamistischen Terrororganisationen Al-Qaida und der sogenannte Islamische Staat verbreiten über das Internet zudem Propaganda-Magazine. Diese enthalten neben politischer Hetze gegen den Westen auch Anleitungen zur Herstellung von Sprengstoff und Bomben sowie zur Durchführung von Terroranschlägen. In den letzten Jahren verlagerten sich die Verbreitungswege islamistischer Propaganda von statischen Internetpräsenzen immer mehr in die Sozialen Netzwerke. Diese sehr schnelllebigen und unmittelbaren Verbreitungswege bedürfen einer intensiven Beobachtung und Auswertung durch die Sicherheitsbehörden. Dies geschieht im LKA NRW in der Staatsschutzabteilung. Das Cybercrime-Kompetenzzentrum wird hier unterstützend tätig, wenn besonderes technisches Wissen gefragt ist. Die immer intensivere Internet-Nutzung dieser Gruppierungen und die ständig neuen Veröffentlichungen stellen auch quantitative Herausforderungen dar. Es gilt, aus der Vielzahl der Informationen relevante Fakten für Gefahrenabwehr und Strafverfolgung herauszufiltern, aber auch zur Erkennung von Strukturen. Diese sind oftmals wesentliche Grundlage für die Einleitung von Straf- und Gefahrenermittlungsverfahren.

Fotos (4): Jochen Tack

Die Hogesa-Demonstration im März 2015 in Wuppertal war in den Wochen zuvor durch die agierenden Interessensgemeinschaften im Internet umfassend beworben worden.

Die Kameradschaft »Division Altenessen« macht bei einer Demonstration auf ihre Internetpräsenz aufmerksam.

Insbesondere die linke Szene nutzt das Internet, um minutenaktuell über Veranstaltungen und das Geschehen vor Ort zu informieren.

Internetauswertung im Kompetenzzentrum Rechtsextremismus

Die rechte Szene nutzt insbesondere die öffentliche Debatte über Zuwanderung für ihre fremdenfeindliche Hetze im Internet. Einige wenige große und überregionale Internetportale richten sich dabei an eine extrem rechte Klientel. Auf regionaler bzw. lokaler Ebene betreiben rechte Parteien, Kameradschaften und andere Gruppierungen ihre Websites mit entsprechender thematischer Aufbereitung. Daneben sind diverse Social-Media-Seiten bedeutsam, insbesondere Facebook, aber auch der russische Betreiber VK.com.

Dementsprechend werten die Staatsschutzdienststellen in den Kriminalhauptstellen das Internet regelmäßig auf regionaler Ebene aus. Bundesweit erfolgt die Auswertung durch die Koordinierte Internet Auswertung-Rechts (KIA-R) des Bundeskriminalamts und des Bundesamts für Verfassungsschutz. Den Erfolg der Auswertung zeigt ein aktuelles Ermittlungsverfahren des LKA NRW: Nachdem die KIA-R wiederholt Propagandadelikte und Volksverhetzungen eines großen überregionalen Portals feststellte, wurde ein Ermittlungsverfahren eingeleitet und mehr als acht Terabyte an Daten von Computern, Smartphones und anderen Datenträgern ausgewertet. Dadurch konnte ein Großteil der Beschuldigten identifiziert werden. Bei der Auswertung wurde die Abteilung Staatsschutz intensiv durch die Expertise des Cybercrime-Kompetenzzentrums unterstützt.

Internetauswertung zu Linksextremismus und Ausländerextremismus

Ebenso wie für den Bereich des Rechtsextremismus erfolgt auch in den Phänomenbereichen Linksextremismus und Ausländerextremismus (ohne Islamismus) eine regelmäßige Internet-Auswertung durch die zuständigen Staatsschutzdienststellen in den Kriminalhauptstellen sowie auf Bundesebene durch das Bundeskriminalamt und das Bundesamt für Verfassungsschutz (Koordinierte Internet Auswertung-Links (KIA-L) und Koordinierte Internet Auswertung Ausländer (KIA-A)). Bereits seit einigen Jahren nutzt insbesondere die linke Szene das Internet vermehrt zur Informationssteuerung und Veranstaltungsmobilisierung. Diverse Social-Media Netzwerke werden bei Veranstaltungen im Minutentakt mit aktuellen Informationen rund um das Geschehen vor Ort gefüttert. Nahezu jede namhafte Organisation bzw. Vereinigung verfügt über teilweise professionell gestaltete Internetportale, welche regelmäßig gepflegt und genutzt werden. ///

Kai-Uwe Kessen, LKA NRW

KOOPERATION

»Gemeinsam gegen Cybercrime«
Vernetzt zum Erfolg

Bereits seit dem Jahr 2011 besteht die »Sicherheitskooperation Cybercrime zur Förderung der Sicherheit bei der Nutzung von Informations- und Kommunikationstechnologien sowie zur präventiven und repressiven Bekämpfung der Cybercrime«. Unter dem Motto »Gemeinsam gegen Cybercrime« haben sich das Landeskriminalamt (LKA) NRW und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) zu diesem Projekt zusammengeschlossen. Der Bitkom-Verband vertritt mehr als 2.000 Unternehmen, davon 1.200 Direktmitglieder mit etwa 700.000 Beschäftigten aus den Bereichen Software, IT-Services, Telekommunikations- und Internetdienste, Computer-Hardware sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Zu den Mitgliedern gehören fast alle Global Player der IT-Branche sowie 800 mittelständische Unternehmen und zahlreiche inhabergeführte Unternehmen.

Die Ziele der Sicherheitskooperation Cybercrime sind
> für die Gefahren von Cybercrime zu sensibilisieren und Bewusstsein zu schaffen
> Erkenntnisse zu neuen Phänomenen zu gewinnen
> die technischen Kompetenzen zu erweitern
> die Prävention fortzuentwickeln
> den Wissenstransfer zur Bekämpfung der Cybercrime zu intensivieren

Die Handlungsfelder der Kooperation sind
> Informationsaustausch und Wissenstransfer
> Gegenseitige Hospitationen
> Dunkelfeldforschung
> Reduzieren des Dunkelfeldes
> Konzeption und Durchführung von Präventionsmaßnahmen
> Vermitteln von Experten in konkreten Einzelfällen


Foto: Bitkom e.V.

Uwe Jacob (Direktor des LKA NRW) und Dr. Thomas Endres (Vorsitzender des Präsidiums des VOICE Bundesverbandes der IT-Anwender e. V.) setzten mit ihren Unterschriften den Grundstein für gemeinsame Präventionsarbeit.


Foto: LKA NRW

LKA NRW KOOPERIERT MIT VOICE BUNDESVERBAND DER IT-ANWENDER e. V.

Einen besseren Anlass hätte es nicht geben können – auf der CeBIT 2015 haben das LKA NRW und der VOICE Bundesverband der IT-Anwender e. V. eine Kooperationsvereinbarung zur präventiven Bekämpfung von Cybercrime unterzeichnet.

Der VOICE Bundesverband der IT-Anwender e. V. umfasst etwa 400 Mitgliedsunternehmen in Deutschland und verfügt über branchenübergreifende Netzwerke, die sich aus den Chief-Information-Officer (CIO) und Fachverantwortlichen der Unternehmen zusammensetzen.

»Ziel der Kooperation ist, das Bewusstsein um die Gefahren der Cybercrime zu verbessern (Awareness), die Prävention fortzuentwickeln und gemeinsame Präventionsmaßnahmen durchzuführen«, sagt Uwe Jacob, Direktor des Landeskriminalamtes NRW, »Im Rahmen dieser Kooperation ist es uns möglich, professionelle IT-Anwender zu erreichen und die polizeiliche Präventionsarbeit bei der Bekämpfung und Verhinderung von Cybercrime effizient zu lenken.«

Unternehmen sollen durch das neu geschaffene Netzwerk besser auf die Zusammenarbeit mit der Polizei in Nordrhein-Westfalen in Fällen von Cybercrime vorbereitet werden. Im Schadensfall lassen sich so wertvolle Informationen und Experten kurzfristig zusammenführen und erforderliche Sofortmaßnahmen einleiten.

Ein konkretes Beispiel der erfolgreichen Kooperation:
Ein Jahr lang haben Ermittler des Landeskriminalamts Nordrhein-Westfalen mit allen zur Verfügung stehenden Mitteln nach einem Kind und dessen Peiniger gefahndet. Der Mann hatte das Kind über Jahre missbraucht und die menschenverachtenden Aufnahmen an Gleichgesinnte im Internet verteilt. Er stellte das Kind weiteren Tätern im wahrsten Sinne des Wortes »zur Verfügung«. Das Kind musste Unsägliches ertragen. Erst als in einem letzten Anlauf Beamte des Landeskriminalamts Nordrhein-Westfalen und Experten aus einem Unternehmen der Sicherheitskooperation Cybercrime gemeinsam völlig neue Taktiken und neue technische Lösungen konzipierten und umsetzten, gelang der Durchbruch: Mehrere Täter wurden in den USA und in Großbritannien identifiziert und festgenommen. Der Junge wurde befreit und befindet sich nun in sicherer Obhut.


Foto: PP Oberhausen

Übten gemeinsam den Ernstfall: Die Teilnehmer des Workshops, bestehend aus Vertretern mehrerer, regionaler Wirtschaftsunternehmen und der Polizei

Workshops mit kleinen und mittelständischen Unternehmen
In der Sicherheitskooperation Cybercrime sollen speziell auch kleine und mittelständische Unternehmen für die Gefahren aus dem Netz sensibilisiert und geschult werden. Dazu wurde unter Koordination des Landeskriminalamts NRW und in Kooperation mit dem Polizeipräsidium Oberhausen sowie dem »Business Partner Club« in Oberhausen, in dem mehrere Unternehmen aus der Region zusammengeschlossen sind, ein Pilotprojekt gestartet: Im Herbst 2013 nahmen 15 IT-Verantwortliche aus den verschiedenen kleinen und mittelständischen Unternehmen im Raum Oberhausen an einem zweitägigen Workshop teil. Ziel des Workshops war es unter anderem, Vertrauen zwischen den ansässigen Wirtschaftsunternehmen und der Polizei vor Ort aufzubauen. »Viele Firmen wenden sich bei Straftaten gegen ihre IT-Systeme – etwa bei Erpressungen – nicht an die Polizei. Sie haben Angst vor schlechter Publicity oder weil sie befürchten, dass die Polizei bei ihren Ermittlungen den laufenden Betrieb behindert. Daher zahlen sie häufig lieber das geforderte Lösegeld«, weiß Mario Lorenz, Organisator des Workshops und Mitarbeiter im Cybercrime-Kompetenzzentrum. Das sei aber der falsche Weg. Nur wenn die Unternehmen mit den Polizeibehörden zusammenarbeiteten, sei es möglich, gegen die Täter vorzugehen.

Die Kooperationspartner im Sicherheitsverbund (von links nach rechts): Uwe Kolmey, Präsident LKA Niedersachsen, Markus Röhrl, Leiter Abteilung 4, LKA NRW, Marc Bachmann, Bitkom e. V., Dieter Schneider, Präsident LKA Baden-Württemberg, Dr. Jörg Michaelis, Präsident LKA Sachsen


FOTO: LKA BW

LKA BADEN-WÜRTTEMBERG, LKA NIEDERSACHSEN UND LKA SACHSEN EBENFALLS MITGLIEDER DER SICHERHEITSKOOPERATION CYBERCRIME

2013 ist das LKA Baden-Württemberg der erfolgreichen Sicherheitskooperation beigetreten. Im Jahr 2014 folgten dann das LKA Niedersachsen und das LKA Sachsen. Andere Bundesländer erwägen, an der Kooperation teilzunehmen. Die einzelnen Partner im Sicherheitsverbund bringen sich dabei mit ihrem spezifischen Wissen ein. »Wir bündeln unsere Kräfte und entwickeln neue Ideen gemeinsam weiter. Dabei gilt es herauszufinden, wer das beste Know-how hat, um ein spezifisches Problem am effizientesten zu lösen«, erklärt Peter Vahrenhorst vom Cybercrime-Kompetenzzentrum NRW. Der Bitkom-Verband und das LKA NRW stehen allen Erweiterungen im Rahmen der Kooperation positiv gegenüber.

Im Rahmen der Veranstaltung wurden verschiedene Angriffs-Szenarien vorgestellt und vor Ort simuliert, zum Beispiel eine DDoS-Attacke oder das Einschleusen eines Trojaners. »Für die Teilnehmer war es durchaus interessant einmal zu sehen, wie so ein Angriff konkret abläuft und selbst ausprobieren zu können, welche Maßnahmen wirksam sein können«, erklärt Lorenz. In weiteren Demonstrationen konnten den Workshop-Teilnehmern auch außergewöhnliche Angriffs-Szenarien anschaulich vermittelt werden: So wurde zwischen einem Rechner und einem Drucker ein kaum sichtbarer Mini-Computer angebracht, der alle Druckaufträge mitzeichnet. »Auch die Themen USB-Sticks und fremde WLAN-Netze wurden angesprochen, da es hier viel Aufklärungsbedarf in den Unternehmen gibt – besonders wenn Beschäftigte häufig mit dem Firmenhandy unterwegs sind«, so Lorenz. >

Fotos (4): Oliver Krato

Digitale Angriffe können ein unverzügliches Handeln der Ermittlungsbeamten des Cybercrime-Kompetenzzentrums erforderlich machen.

Zwei Kriminalbeamte des Polizeipräsidiums Oberhausen beleuchteten im Anschluss das polizeiliche Vorgehen von der Anzeigenerstattung bis zur Gerichtsverhandlung. »Es war uns wichtig, dass die Unternehmen einen Einblick in unsere Arbeit bekommen und zum Beispiel über die forensische Auswertung der Daten Bescheid wissen – so konnten bei den Workshop-Teilnehmern viele Hemmschwellen abgebaut werden«, ist sich Mario Lorenz sicher. Tipps zur Prävention schärften den Blick für mögliche Angriffs-Szenarien und sorgten für angeregte Diskussionen.

Künftig soll es weitere Kooperationen mit anderen Behörden in NRW geben. »Wir möchten auch weiterhin den Austausch zwischen Polizei und Wirtschaftsunternehmen fördern. Daher arbeiten wir daran, diese Workshops als eine Art Baukastensystem anzubieten, damit die Behörden möglichst wenig Aufwand mit der Organisation einer solchen Veranstaltung haben«, erklärt Mario Lorenz.

Hospitationen

Im Rahmen der Sicherheitskooperation Cybercrime werden über gegenseitige Hospitationen zwischen Polizei und der Wirtschaft wertvolles Wissen und langjährige Erfahrungen ausgetauscht. Bei den Hospitationen wechselt jeweils ein Mitarbeiter für mehrere Wochen seinen Arbeitsplatz – Kooperationen in diesem Bereich gab es bislang zum Beispiel mit den Unternehmen IBM und Capgemini in den Bereichen Analyse von großen Datenmengen und der Vereinfachung von Geschäftsprozessen. Weitere Hospitationen sind bereits geplant. »Diese Hospitationen sind besonders wichtig für uns, weil wir vor ermittlungstechnischen Problemen stehen, die wir durch den Einkauf technischer Produkte nicht lösen und durch eigene Fortbildungen nicht abdecken können«, erklärt Peter Vahrenhorst vom Cybercrime-Kompetenzzentrum. Mithilfe der Wirtschaftsunternehmen aus der Sicherheitskooperation Cybercrime kann diese Wissenslücke geschlossen werden.

Kritische Infrastrukturen schützen

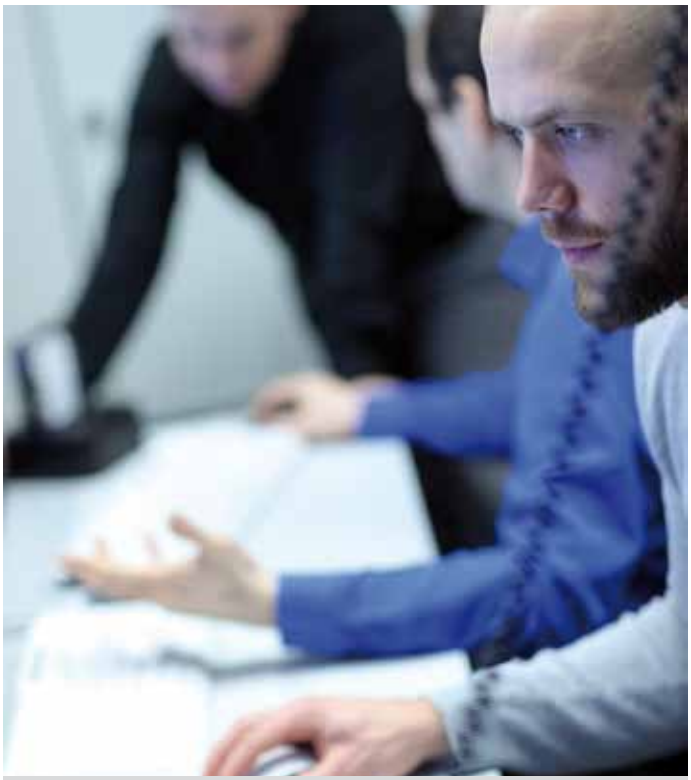
Kritische Infrastrukturen sind Systeme, die für das Funktionieren unserer Gesellschaft unerlässlich sind und deren Ausfall erhebliche Auswirkungen auf das Allgemeinwohl mit sich bringen würden – wie etwa Elektrizitäts- oder Wasserwerke, aber auch Krankenhäuser oder das Verkehrswesen. Innerhalb der Sicherheitskooperation Cybercrime beschäftigt man sich seit Jahren mit diesem wichtigen Thema, denn auch wenn es bislang noch keine Angriffe in diesem Bereich gab, die größere Auswirkungen auf die Gesellschaft hatten, sind solche Attacken technisch denkbar. »Man muss sich frühzeitig auf derartige Szenarien vorbereiten, denn wenn es soweit ist, wird es schwierig sein, noch adäquat reagieren zu können. Die Konsequenzen eines solchen Angriffs können fatal sein – etwa, wenn man an langandauernde und großflächige Stromausfälle denkt, weil die Steuerungsanlagen von Elektrizitätswerken lahmgelegt werden«, erklärt Helmut Picko vom Cybercrime-Kompetenzzentrum. Das Vorgehen allein mit polizeilichen Mitteln würde bei einem großangelegten Angriff nicht ausreichen. Daher ist eine enge Zusammenarbeit mit allen Beteiligten unerlässlich. Schon im Vorfeld müssen sämtliche Protagonisten einbezogen werden. Dazu gehören die Zentralstellen von Bund und Ländern, wie etwa die Landeskriminalämter, die Feuerwehr, der Katastrophenschutz, aber auch die Kommunen, die verschiedenen

Telekommunikationsanbieter oder potenziell betroffene Unternehmen. »Die Schnittstelle zur Wirtschaft ist hier besonders wichtig, denn wir können uns nur erfolgreich gegen derartige Angriffs-Szenarien wappnen, wenn wir gemeinsam die erforderlichen Maßnahmen planen. Dazu bietet die Sicherheitskooperation Cybercrime die entsprechende Plattform, so dass im Ernstfall jeder weiß, was zu tun ist. Nur so bleiben wir handlungsfähig«, betont Helmut Picko.

ZISC

Das Zentrale Informations- und Servicezentrum Cybercrime (ZISC), Sachgebiet 41.2 im LKA NRW, gewährleistet den Informationsaustausch mit den Polizeibehörden des Landes NRW und mit polizeilichen Zentralstellen des Bundes und der Länder im Zusammenhang mit der Bekämpfung von Cybercrime. Die Mitarbeiter des ZISC stehen auch externen Behörden, Institutionen und der Wirtschaft als zentrale Ansprechstelle Cybercrime zur Verfügung. Dafür wurde eigens ein Single Point of Contact (SPOC) eingerichtet, der 24/7 erreichbar ist.

»Grundsätzlich ist der SPOC dazu da, Anfragen oder Anzeigen entgegenzunehmen, selbst zu bearbeiten oder an die entsprechenden Stellen weiterzuleiten – und das 24 Stunden am Tag«,



24 Stunden am Tag erreichbar: Der Single Point of Contact

Mitarbeiter des Cybercrime-Kompetenzzentrums im Einsatz

erklärt Wolfgang Holzapfel vom Cybercrime-Kompetenzzentrum. Unternehmen melden sich häufig beim Single Point of Contact, weil es einen konkreten Sicherheitsvorfall gegeben hat und sie angegriffen wurden – etwa, wenn Cyberkriminelle interne Daten abgeschöpft haben oder das Unternehmen erpresst wurde. »Weil wir rund um die Uhr erreichbar sind, können wir auf solche Vorfälle schnell reagieren und die betroffenen Unternehmen umgehend mit entsprechenden Maßnahmen unterstützen«, so Holzapfel. Dazu stehen Teams zur Datensicherung und Forensiker zur Analyse der Daten bereit. »Wir treffen die nötigen Sofortmaßnahmen und bewerten den Fall nach seinem Ermittlungsumfang und seiner Brisanz. Danach wird entschieden, ob der Fall an die zuständige Kreispolizeibehörde abgegeben oder im LKA NRW eine eigene Ermittlungskommission eingerichtet wird.« Dabei kümmern sich die Mitarbeiterinnen und Mitarbeiter auch um generelle Anfragen rund um das Thema Cybercrime und Sicherheit von Unternehmen oder auch aus Behörden. Dabei stehen Anfragen zu speziellen Technologien wie Anonymisierung oder Verschlüsselung, aber auch zu bestimmten Soft- oder Hardwareprodukten im Mittelpunkt. Für solche Anfragen steht der SPOC des LKA NRW auch mit dem zentralen SPOC des Bitkom-Verbandes mit seinen 2.000 IT-Unternehmen sowie mit den SPOC der kooperierenden Landeskriminalämter in Kontakt. »Über diese Vernetzung versuchen wir, schnell den bestmöglichen Lösungsansatz für das jeweilige Problem zu finden«, so der Experte. /// ***Simone Wroblewski***


Foto: Jochen Tack

CYBERCRIME-BEKÄMPFUNG

International, anonym und gut verschlüsselt
Polizeiarbeit mit Hindernissen

Bei der Bekämpfung von Cybercrime steht die Polizei vor großen Herausforderungen: Täter agieren international und nutzen technische Möglichkeiten, um sich im Netz anonym zu bewegen und ihre Daten zu verschlüsseln. Auch die bislang fehlende Vorratsdatenspeicherung erschwert die Ermittlungen im Bereich Cybercrime enorm. Welche Ermittlungshemmnisse spielen beim Thema Cybercrime eine Rolle und welche Maßnahmen können dazu beitragen, die Cybercrime-Bekämpfung effektiver zu gestalten?

Nationale Grenzen existieren im Internet nicht und somit auch nicht für Cyberkriminelle. Insbesondere organisierte Tätergruppen mit kommerziellen Zielen sowie Hacker-Kollektive wie »Anonymous« agieren international. Zudem nutzen viele Täter Anonymisierungsmethoden, die den Datenverkehr über weltweit verteilte Server umleiten. Damit führen polizeiliche Ermittlungen immer häufiger und schneller zu digitalen Spuren, die nur noch im Ausland weiterverfolgt werden können. Der Ermittlungserfolg hängt dann von vielen Faktoren ab. Die erforderlichen Daten internationaler Konzerne können beispielsweise von ausländischen Niederlassungen rechtmäßig ins Inland übermittelt werden, wo ein Zugriff mittels eines deutschen richterlichen Beschlusses möglich ist. In anderen Fällen bleibt hingegen lediglich der Weg über polizeiliche oder justizielle Rechtshilfeersuchen. Die Erfolgsaussichten richten sich dann nicht nur nach den jeweiligen Rechtshilfeabkommen, sondern auch nach der Leistungsfähigkeit und -willigkeit der ausländischen Ermittlungsbehörden.

Cybercrime-Convention als gemeinsame Rechtsgrundlage

Für die spezifischen grenzüberschreitenden Ermittlungsmaßnahmen sind Rechtsgrundlagen, die über die Strafprozessordnung (StPO) hinausgehen, erforderlich. Eine solche Ermächtigungsgrundlage stellt das »Übereinkommen über Computerkriminalität« (Cybercrime-Convention) vom 23. November 2001 dar. Diese Vereinbarung wurde bislang von 39 Mitgliedsstaaten des Europarates und sechs Nicht-Mitgliedern des Europarates ratifiziert und in Kraft gesetzt.

In Bezug auf die Cybercrime-Convention muss differenziert werden, wie in der jeweiligen Nation verfahren wird, wenn der Staat zwar die Cybercrime-Convention unterzeichnet hat, aber die Umsetzung in nationales Recht (noch) nicht erfolgt ist. Bei der Planung entsprechender Ermittlungsmaßnahmen kann auf die Informationen des Infopools IPZ (Internationale polizeiliche Zusammenarbeit) zugegriffen werden, um eine differenzierte Darstellung der Rechtslage und konkrete Informationen zu den einzelnen Nationen zu erhalten.

BKA ist in Deutschland zentrale Ansprechstelle

Im Rahmen der grenzüberschreitenden Zusammenarbeit auf Basis der Cybercrime-Convention ist für Deutschland das BKA bei der Übermittlung der Informationen und Ersuchen zwingend zu beteiligen. Der Schriftverkehr ist demnach über das LKA NRW als Prüfungs- und Bewilligungsbehörde an das BKA zu richten. Beim BKA wird diese Aufgabe durch die Fachdienststelle SO 43 wahrgenommen (§ 3 (2) BKAG i. V. m. Nr. 123, 124 RiVASt-Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten). Bei der Vorbereitung entsprechender Ermittlungsmaßnahmen sollte sich die ermittlungsführende Behörde mit dieser Dienststelle des BKA in Verbindung setzen, um landesspezifische Gegebenheiten und Verfahrensweisen zu erfragen und abzustimmen.

Die Dienststelle SO 43 ist die nach Artikel 35 Cybercrime-Convention zu bestimmende G8-Kontaktstelle für Deutschland. Sie unterstützt grenzüberschreitende Ermittlungen auch außerhalb der Bürodienstzeiten durch:

> fachliche Beratung,
> Sicherung von Daten nach den Artikeln 29 und 30 Cybercrime-Convention
> Erheben von Beweismitteln, Erteilen von Rechtsauskünften und weiteren Unterstützungshandlungen.

Cyberkriminelle nutzen Anonymisierungspotenziale

Den im Internet agierenden Tätern ist häufig bewusst, dass sie über ihre IP-Adresse identifiziert werden können. Um dies zu vermeiden, nutzen sie verschiedene Möglichkeiten der Anonymisierung, beispielsweise durch Umleitung des Datenverkehrs über zwischengeschaltete Server. Anbieter sogenannter Virtual Private Network (VPN)-Dienste werben damit, die Datenübertragung zwischen dem Computer des Benutzers und dem jeweiligen Ziel im Internet verschlüsselt über ihre im Ausland befindlichen Server umzuleiten und keine eigene Protokollierung vorzunehmen. Eine darüber hinaus häufig genutzte Form der Anonymisierung erfolgt über das »The Onion Router« (TOR)-Netzwerk. Dieser kostenlose Dienst besteht aus einer Vielzahl von weltweit verteilten Servern,

@ Eine aktuelle Auflistung der Nationen, die die Cybercrime-Convention anwenden, gibt es auf der Homepage des Europarates: http://conventions.coe.int

Foto: Jan Potente

über die die Datenpakete geleitet werden. Beim Verbindungsaufbau wird durch das Programm eine zufällige Route über einen Teil dieser Server festgelegt. Die Server führen dabei keine Protokollierung über Herkunft oder Ziel der Daten durch. Das TOR-Netzwerk wird daher von Kriminellen gern zur Identitätsverschleierung genutzt, um so die Strafverfolgung zu erschweren.

Über das TOR-Netzwerk erfolgt zum Beispiel auch der Zugang zum sogenannten Darknet. Darknet oder »Hidden Services« sind versteckte Subnetze des Internets, die die Identität des Nutzers verbergen. Sie bieten Kriminellen die Möglichkeit, innerhalb anonymer Serverstrukturen, wie denen des TOR-Netzwerks, Internetseiten zu betreiben, deren Inhalte zwar angezeigt, deren tatsächlicher Standort jedoch nicht über die IP-Adresse ermittelt werden kann. Diese Möglichkeit nutzen Kriminelle, um beispielsweise illegalen Handel mit Drogen zu betreiben oder für die Verbreitung kinderpornografischen Materials. Dies führt dazu, dass die Täter nicht oder nur mit einem erheblich höheren Aufwand ermittelt werden können. >

Foto: Jochen Tack

Der Sperrcode im Handy – Ein Schutz, der nicht immer zum Vorteil der polizeilichen Ermittlungsarbeit ist

Passwortschutz und Kryptierung erschweren die Untersuchung von Datenträgern

Neben Anonymisierungsmethoden nutzen Cyberkriminelle auch passwortgeschützte Zugänge und Verschlüsselungstechniken, die sogenannte Kryptierung, um forensische Untersuchungen von Daten und Datenträgern durch die Polizei zu verhindern. Kryptierung stellt damit ein weiteres Ermittlungshemmnis dar, ist aber zugleich auch ein Sicherheitsfeature und Teil des Datenschutzes. Im Sachgebiet 43.1 »Landeszentrale IuK-Ermittlungsunterstützung« des LKA NRW werden digitale Systeme untersucht, die mutmaßlich verfahrensrelevante Daten beinhalten, jedoch durch einen Zugriffsschutz gesichert wurden. Das kann bei bestimmten Smartphones mit Sperrcode der Fall sein oder bei Laptops, die nur nach Eingabe eines Passworts hochfahren. Arbeitet der Beschuldigte nicht mit den Ermittlern zusammen und hält er das Passwort unter Verschluss, kann das unter bestimmten Umständen dazu führen, dass die Daten – und damit Beweise – tatsächlich verborgen bleiben.

Verschlüsselt werden können Datenträger wie Festplatten, USB-Sticks, der Speicher von Smartphones oder einzelne Dateien. Dabei werden die lesbaren Daten, wie zum Beispiel Bilder oder Textdokumente, mit einem Passwort in ein Chiffrat, das heißt einen verschlüsselten Text, überführt. Im Idealfall lässt das Chiffrat keine Schlüsse auf die Originaldaten zu und die verwendete Verschlüsselungsmethode verfügt über keine Sicherheitslücken, so dass ausschließlich mit dem zugehörigen Schlüssel entschlüsselt werden kann.

Da hilft nur Ausprobieren – Verschlüsselungsmethode AES

Als Verschlüsselungsmethode wird heutzutage häufig AES (»Advanced Encryption Standard«) verwendet. Der zugrunde liegende Algorithmus »Rijndal« wurde von zwei belgischen Kryptologen entwickelt. AES gilt als sicher; als einzige wirksame Angriffsmöglichkeit gegen ein Chiffrat gilt nur das Ausprobieren aller Schlüssel. Da AES mindestens Schlüssel mit einer Länge von 128 Bit verwendet, sind damit etwa 340 Sextillionen, in Zahlen 340.000.000.000.000.000.000.000.000.000.000.000 Entschlüsselungsversuche notwendig, um alle Schlüssel auszuprobieren. Ein 128 Bit AES-Schlüssel kann wie folgt aussehen: ECC56555A7E9ABC55E36941B3D856737. Weil dieser in dieser Form zu abstrakt und komplex ist, erzeugt ein Zwischenschritt – die sogenannte Passwortableitungsfunktion – aus einem »lesbaren« Passwort des Nutzers diesen Schlüssel. Möchte man ein Chiffrat ohne Kenntnis des Passworts entschlüsseln, ist es angesichts der oben genannten riesigen Anzahl möglicher Schlüssel einfacher, alle Passwörter »aaaaa bis zzzzz« durchzuprobieren, anstatt alle Schlüssel. Die Anzahl der möglichen Passwortkombinationen hängt von der Passwortlänge und dem Zeichenvorrat wie Groß- und Kleinbuchstaben, Ziffern oder Sonderzeichen ab. Eine vollwertige Tastatur ermöglicht etwa 100 verschiedene Zeicheneingaben. Mit einem einstelligen Passwort sind daher 100 verschiedene Passwörter auszuprobieren, bei zwei Stellen sind es 10.000, bei drei Stellen 1.000.000 (eine Million), bei neun Stellen 1.000.000.000.000.000.000 (eine Trillion) usw.

Grafikkarten als Hilfsmittel

Wie schnell nun ein Passwort herausgefunden werden kann, hängt davon ab, wie viele Passwörter ein Rechner pro Zeiteinheit gegen das Chiffrat testen kann. Je mehr Rechenleistung vorhanden ist, desto schneller geht die Prüfung vonstatten. Hier gibt es verschiedene interne und externe Möglichkeiten, auf die das LKA NRW zurückgreifen kann. Grafikkarten haben sich dabei als Hilfsmittel zur Prüfung als besonders geeignet herausgestellt. Diese Computerbauteile dienen eigentlich dazu, ein Bild auf den Monitor zu bringen. Die darin verwendeten Grafikprozessoren bestehen aus tausenden Recheneinheiten, die entwickelt wurden, um mehrere Aufgaben gleichzeitig zu lösen. Sie sind damit bestens geeignet, gleich mehrere Passwörter parallel zu verarbeiten. Dieses so genannte »GPU-Computing« wird im LKA NRW schon lange betrieben und weiter ausgebaut. Kurzfristig könnten auch dezentrale Rechenkapazitäten aus mehreren Rechenzentren zugemietet werden, um den Prozess weiter zu beschleunigen. Die Erfahrungen aus solchen Ermittlungsansätzen werden auf dem vom BKA organisierten, jährlich stattfindenden »Sachbearbeitertreffen Kryptoanalyse« ausgetauscht.

Fehlende Vorratsdatenspeicherung kann Ermittlungen unmöglich machen

Aufgrund fehlender Mindestspeicherfristen von Verkehrsdaten zur Telekommunikation (umgangssprachlich Vorratsdatenspeicherung) stehen die für die polizeilichen Ermittlungen erforderlichen Daten als oftmals einzige Ermittlungsansätze in vielen Fällen erst gar nicht zur Verfügung. Während die relevanten Daten von einigen Unternehmen für wenige Tage gespeichert werden, wird

DAS URTEIL DES EUROPÄISCHEN GERICHTSHOFS ZUR VORRATSDATENSPEICHERUNG

Mit Urteil vom 8. April 2014 erklärte der EuGH die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten für ungültig.
Die Richtlinie sah vor, Daten zu speichern, aus denen zu entnehmen war, mit welcher Person ein Teilnehmer auf welchem Weg kommuniziert hat, wie lange die Kommunikation gedauert hat, von welchem Ort aus sie stattfand und wie häufig der Teilnehmer während eines bestimmten Zeitraums mit bestimmten Personen kommuniziert hat. Die Speicherung des Inhalts elektronischer Kommunikation war nicht Gegenstand der Richtlinie.
In seiner Entscheidung verdeutlichte der EuGH, dass die Richtlinie den Wesensgehalt der Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten nicht angetastet hat. Sie diene darüber hinaus dem Gemeinwohl, d. h. der Bekämpfung schwerer Kriminalität und somit letztlich der öffentlichen Sicherheit.
Dennoch erklärte er die Richtlinie für ungültig, da sich die mit den Regelungen einhergehenden Grundrechtseingriffe nicht auf das tatsächlich absolut Notwendige beschränken, und somit der Grundsatz der Verhältnismäßigkeit nicht genügend beachtet werde. Der EuGH führte folgende Gründe für seine Entscheidung an:

- **Es gab keine Differenzierung, Einschränkung oder Ausnahme hinsichtlich der elektronischen Kommunikationsmittel und Verkehrsdaten sowie des Personenkreises.**
- **Es wurden keine objektiven Kriterien hinsichtlich der Straftaten festgelegt, bei denen ein Zugang zu den gespeicherten Daten möglich sein soll.**
- **Es fehlten objektive Kriterien, die gewährleisten, dass der Zeitraum der Datenspeicherung auf das Notwendigste beschränkt wird.**
- **Es lagen keine verbindlichen Regelungen für die Diensteanbieter zum Schutz vor Missbrauch der gespeicherten Daten und unberechtigtem Zugang vor.**
- **Es fehlten Bestimmungen, dass die gespeicherten Daten auf dem Gebiet der EU vorgehalten und dass Datenschutz und -sicherheit durch unabhängige Stellen überwacht werden.**

Die EU-Kommission kann die Vorgaben des EuGH in einer neuen Richtlinie umsetzen. Hiervon unabhängig kann Deutschland aber auch eine eigene Regelung zur Vorratsdatenspeicherung einführen. Zahlreiche der vom EuGH bemängelten Defizite waren in der vom BVerfG am 2. März 2010 für nichtig erklärten früheren deutschen Regelung zur Vorratsdatenspeicherung bereits berücksichtigt bzw. hätten in einer neuen Fassung berücksichtigt werden können.

@ **Das Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung:** http://curia.europa.eu

von anderen auf die Speicherung völlig verzichtet. Trotz umfangreicher Ermittlungen ist dann eine Identifizierung des Täters oft nicht oder nur mit einem erhöhten zeitlichen, technischen und personellen Arbeitsaufwand möglich. Ein Beispiel: Im Zuge der Auswertung eines Rechners, über den Kinderpornografie verbreitet worden war, wurde 2014 festgestellt, dass der Beschuldigte über den Kommunikationsdienst ICQ mit 146 Personen Kinder- bzw. Jugendpornografie getauscht hatte. Letztlich konnten nur 35 Tatverdächtige namentlich ermittelt werden. In 111 Fällen (76 Prozent) gelang es nicht, die Tatverdächtigen zu ermitteln. Aufgrund fehlender oder unzureichender Speicherungsfristen konnten über die Internetservice-Provider keine Daten erhoben werden. Ein weiteres Problem für die Ermittler war, dass die E-Mail Provider auf eine Personendatenverifizierung in der Regel ganz verzichten.

Notwendige Schritte zur erfolgreichen Cybercrime-Bekämpfung

Besonders für die aufwändigen Ermittlungen im Bereich Cybercrime, aber auch für andere Kriminalitätsphänomene und zur Bekämpfung des Terrorismus, ist das Vorhalten von Telekommunikationsverkehrsdaten erforderlich, um schwerste Kriminalität erfolgreich bekämpfen zu können. Aufgrund der aktuellen Entscheidung des Europäischen Gerichtshofs zur Vorratsdatenspeicherung ist Deutschland nunmehr gefordert, eine rechtstaatliche Lösung herbeizuführen und sich auf europäischer Ebene einzubringen.

So wenig wie Cybercrime an nationale Grenzen gebunden ist, so wenig sollten polizeiliche Ermittlungen im Bereich Cybercrime an nationale Grenzen gebunden sein. Internationale Vereinbarungen wie die Cybercrime-Convention stellen einen wichtigen Schritt in der Bekämpfung von Cybercrime dar und müssen erweitert, vertieft und umgesetzt werden. Ermittlungshemmnissen wie Internationalisierung, Anonymisierung und Kryptierung kann nur mit organisatorischen, personellen und technischen Maßnahmen auf Seiten der Strafverfolgungsbehörden begegnet werden. Hierbei wird mit einem erhöhten zeitlichen, technischen und personellen Aufwand zu rechnen sein. Die Polizei Nordrhein-Westfalens hat in der Bekämpfung der Cybercrime einen strategischen Schwerpunkt gesetzt. Durch Kooperationen mit Wirtschaft, Forschung und Lehre findet das LKA NRW neue Partner in der Cybercrime-Bekämpfung und erschließt so innovative Ermittlungsansätze und -instrumente. /// ***Nadja Kwasny, LKA NRW***

IT-Fortbildungen beim LAFP

Von Einsteigerseminaren bis Expertenschulungen

Im Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten (LAFP) NRW sind für das Jahr 2016 über 40 Seminare alleine im Bereich der Informationstechnologie (IT) geplant. Manche dauern nur einen Tag, andere vier Wochen. Der Bedarf im Land ist eigentlich noch höher.

Foto: Jochen Tack

»Doch mit dem vorhandenen Personal und den Räumlichkeiten ist mehr einfach nicht zu machen«, berichtet Thomas Jansen, Leiter des Sachgebietes 22.2 IuK-Kriminalität, IuK-Forensik, TKÜ. »Im bundesweiten Vergleich stehen wir damit aber noch gut da«, sagt er. Die Lehrenden unterrichten nicht nur bei den zahlreichen Seminaren ihres Sachgebietes, sondern sind auch bei vielen anderen Fortbildungen im Einsatz, denn digitale Spurensicherung ist fast überall ein Thema. Die Fortbildungen im IT-Bereich sind sehr breit gefächert. Sie reichen von Einsteigerseminaren bis hin zu Fortbildungen für Experten, etwa im Bereich der Netzwerkforensik oder der skriptbasierten Auswertung.

Voraussetzung für alle weiteren Seminare ist die vierwöchige Einführungsfortbildung »IT-Forensik Grundlagen«. Dadurch soll sichergestellt sein, dass alle Teilnehmer über das gleiche Grundwissen verfügen. Am Ende dieser vier Wochen können die Teilnehmer etwa eine Durchsuchung planen und durchführen, Datenträger sicherstellen, sie auswerten und so aufbereiten, dass sie vor Gericht verwendet werden können. Auch rechtliche Grundlagen werden vermittelt. Dabei steht neben der Theorie immer auch die Praxis im Vordergrund. Am Ende dürfen dann alle ihr Wissen bei mehreren praktischen Übungen unter Beweis stellen.

Florian Siegert vom Landrat Lippe ist schon seit 2012 in dem Bereich IT-Ermittlungsunterstützung tätig. Er hat die Einführungsfortbildung vor allem belegt, um anschließend die Spezialkurse besuchen zu dürfen. »Ich fand die Tipps und Tricks, die man hier erhält, hilfreich«, berichtet er, »so habe ich noch einiges mitnehmen können, wenn es darum geht, wie man Berichte allgemeinverständlich verfasst.« Er freut sich auch, dass er in den Lehrenden den Ansprechpartner für die Zukunft kennengelernt hat.

Man muss ständig am Ball bleiben

Das Grundlagenseminar wird grundsätzlich immer von zwei Lehrenden begleitet, damit sichergestellt ist, dass alle Teilnehmer entsprechend ihrer Vorkenntnisse betreut werden können. Sebastian Schlepphorst ist einer der Lehrenden bei der Einführungsfortbildung. Er ist

Sebastian Schlepphorst (rechts im Bild) erklärt Seminarteilnehmer Florian Siegert die Live-Forensik.

Fotos (2): Ralph Lueger

Der Lehrende Heiko Wolter vermittelt anschaulich theoretisches Wissen zum Deliktsbereich Cybercrime.

der Jüngste im Team. Der 25-Jährige hat erst vor kurzem von der Landespolizei Brandenburg nach Nordrhein-Westfalen gewechselt. Trotz seiner jungen Jahre hat er schon einiges an Erfahrung sammeln und internationale Kontakte, die sich während seines berufsbegleitenden Studiums in Dublin zum Master of Science „Forensic Computing and Cybercrime Investigation" ergeben haben, knüpfen können.

Veränderungen und aktuelle Phänomene der Delikte Cybercrime erfordern ständige Innovation und Weiterentwicklung auch in der Fortbildung. »Wir müssen als Lehrende ständig am Ball bleiben und uns fachlich fit halten – auch in der Freizeit«, sagt Heiko Wolter, ein weiterer Lehrender, »schließlich wollen die Lernenden ständig aktuelle Informationen haben.«

Multiplikatoren tragen Wissen in die Behörden

Die weiteren Anpassungsfortbildungen beinhalten zum Beispiel auch betriebsspezifische Lehrgänge zu Windows, Linux und Mac-Computern. »Apple-Fortbildungen in dieser Tiefe bieten, soweit ich weiß, in Deutschland nur wir an, da wir die entsprechende Mac-Umgebung haben«, berichtet Thomas Jansen, der ab Sommer 2015 seinen Dienst im Cybercrime-Kompetenzzentrum des LKA NRW versehen wird. Schließlich sollten die Teilnehmer wissen, wo bei dem jeweiligen Betriebssystem die für die Polizei relevanten Informationen abgelegt werden.

»Unsere Aufgabe ist es, IT-Know-how in die Fläche zu bringen«, berichtet der Sachgebietsleiter. Daher fanden im November 2014 erstmals zehn eintägige Seminare statt, in denen die unmittelbaren Möglichkeiten für Polizeibeamte erläutert wurden, wenn über die Notrufnummer 110 Informationen eingehen, die einen Bezug zum Internet haben. Geschult wurden Multiplikatoren, die ihr Wissen dann in die jeweiligen Behörden weitertragen. Drei weitere Module werden zeitnah folgen. ///

Katerina Breuer

Foto: Jochen Tack

LKA-TIPPS ZUR SICHERUNG DIGITALER SPUREN

Bei jedem Einsatz können plötzlich unerwartet digitale Spuren auftauchen. Wie man am besten reagiert und an wen man sich bei Fragen wenden kann, zeigen die folgenden Tipps:

> Den weiteren Zugriff von Beschuldigten/Zeugen auf alle Geräte wie PC, Laptop, Smartphone und Tablet verhindern.

> Den Zustand der digitalen Geräte ermitteln und beibehalten: Ist das Gerät ausgeschaltet, nicht einschalten und umgekehrt. Wenn das Gerät eingeschaltet ist, im Zweifelsfall die Kriminalwache oder die Cybercrime-Fachdienststelle verständigen. Smartphones und Tablets in den Einstellungen in den Flugmodus versetzen und Bildschirmsperren verhindern.

> Nach potenziellen externen Datenträgern suchen, beziehungsweise diese erfragen. Das können neben USB-Sticks und Festplatten auch Cloud-Dienste sein oder weitere über das WLAN eingebundene Geräte. Zu bedenken ist, dass USB-Sticks und Speicherkarten in ihrem Aussehen vielfältig sein können und oft nicht auf den ersten Blick als solche zu erkennen sind. Sie können etwa als alltägliche Gebrauchsgegenstände getarnt sein.

> Für die Beweissicherung sind Fotos vom aktuellen Status der digitalen Geräte notwendig (bei Fotos von Bildschirminhalten möglichst ohne Blitzlicht). Dazu gehören Bilder von allen Seiten, auf denen auch die angeschlossenen Geräte und der Bildschirm sichtbar sind. Die Systemzeit mit Abgleich zur aktuellen Tageszeit sollte festgehalten werden. Gibt es hier Abweichungen, sollten diese dokumentiert werden.

> Wenn digitale Geräte sichergestellt werden, ist auch an die dazugehörigen Netzteile beziehungsweise Ladegeräte zu denken.

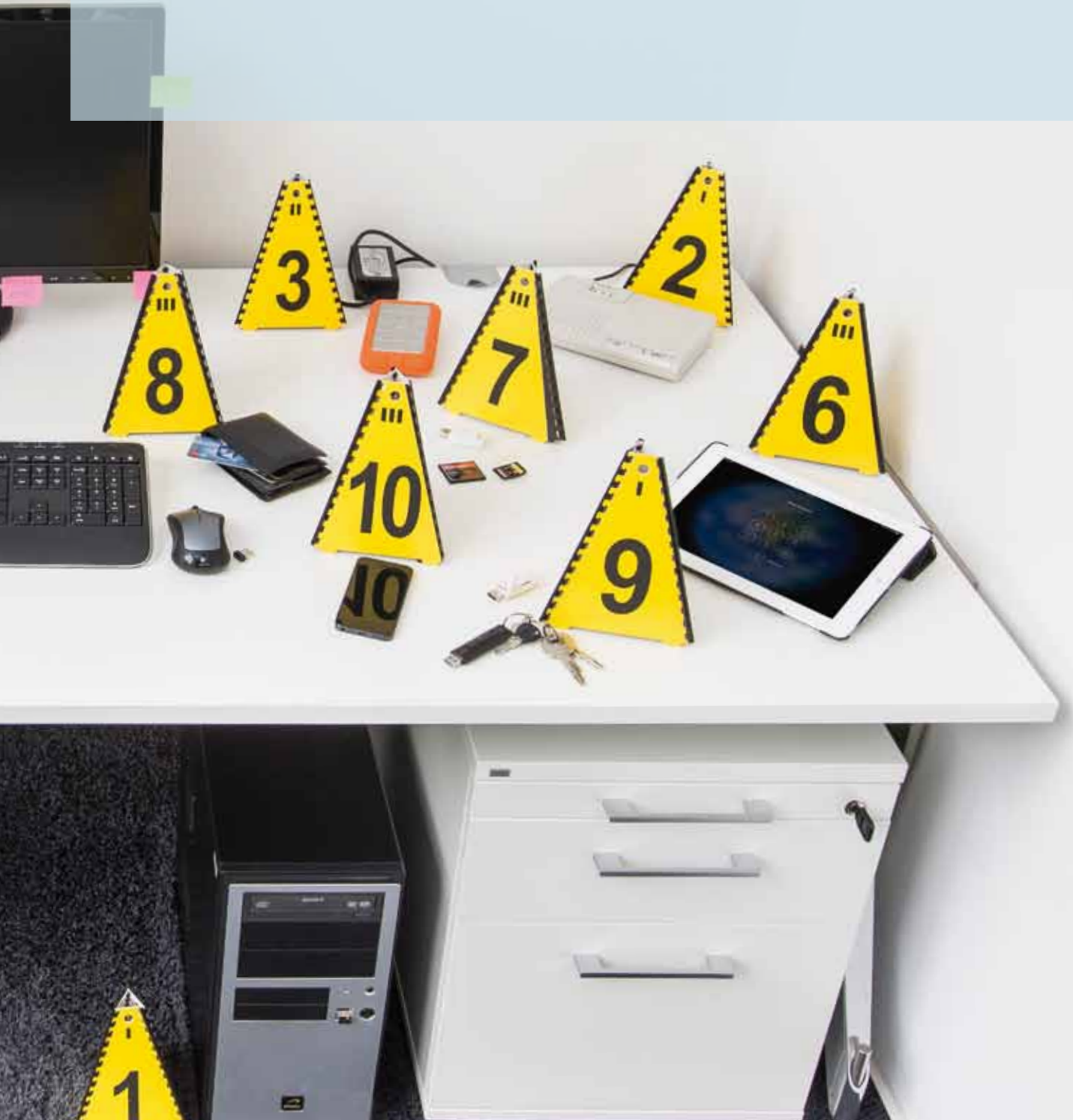
> Für eine spätere forensische Auswertung der Geräte können Passwörter wichtig sein. Daher sollten Zugangsdaten wie PIN, PUK und Passwörter direkt vor Ort erfragt werden genauso wie Zugriffsberechtigungen für weitere Nutzer. Darüber hinaus sollte am gesamten Tatort nach möglichen Notizen von Passwörtern gesucht werden.

> Vor Ort sollte der Beschuldigte/Zeuge auch bezüglich der Nutzung Sozialer Netzwerke befragt werden. Entsprechende Zugangsdaten sollten erfasst werden.

> Nach Sicherstellung sollte ein Einverständnis zur Durchsicht der Daten eingeholt werden (§ 110 StPO).

> Sollten im Anschluss weitere Ermittlungen/Recherchen im Internet erforderlich sein, sollte der Zugang immer über einen freien Internetrechner erfolgen – und nicht über einen CNPol-Rechner.

> Auch für digitale Spuren gelten die Regeln der analogen Beweissicherung. Wichtig ist, die getroffenen Maßnahmen umfassend zu dokumentieren, zu fotografieren und die gesamten Lebensumstände zu erfassen, so dass alle Maßnahmen im Detail nachvollzogen werden können.



Präventionsfilme »Sichere Netzwelten«

Bewusstsein schaffen für Cybermobbing, Datenklau und Passwort-Phishing

Kaum ein Thema ist so komplex wie Cybercrime und kaum ein Bereich betrifft so viele Menschen gleichermaßen. Von Schülern bis zu Senioren, vom Privathaushalt über kleine und mittelständische Unternehmen bis hin zu großen Behörden – jeder sollte sich darüber Gedanken machen, wie er sich vor Angriffen schützen kann. Aber wie erreicht man die unterschiedlichen Zielgruppen, damit sie überhaupt ein Risikobewusstsein für die Gefahren im Netz entwickeln? Der Landespräventionsrat NRW hat unter Koordination des Cybercrime-Kompetenzzentrums eine Reihe von Videos konzipiert. Die Filme thematisieren die vielfältigen Cybercrime-Phänomene und bereiten sie zielgruppenspezifisch auf.

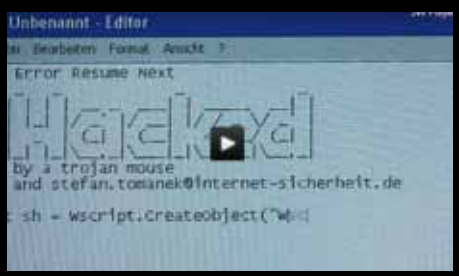
DER LANDESPRÄVENTIONSRAT NRW

Im Juli 2002 wurde in Nordrhein-Westfalen erstmals ein Landespräventionsrat (LPR) eingerichtet. Seine Arbeit soll dazu beitragen, Kriminalitätsphänomene zu erfassen, sie öffentlich sichtbar zu machen und Gegenstrategien zu entwickeln. Grundlage sind aus der Wissenschaft und Praxis gewonnene Erkenntnisse und Erfahrungen über Präventionskonzepte und -projekte. Aus dieser Sicht berät der LPR die Landesregierung. In der Praxis bedeutet das vor allem, Fragen zu stellen: Wie entstehen bestimmte Kriminalitätsphänomene und wie können diese verhindert werden? Wie kann in einem Stadtteil, in dem eine Hochhausfassade an die nächste grenzt, wieder ein gemeinsames Miteinander entstehen, ohne Angst vor Gewalt und dem Wunsch alles zu zerstören? Wie kann man die Menschen für Gefahren im Umgang mit neuen Medien sensibilisieren, ohne von der Nutzung dieser Kommunikationsmittel abzuschrecken? Der LPR NRW entwickelt Strategien, um sich diesen und ähnlichen Problemfeldern aus unterschiedlichen Richtungen zu nähern, um Strukturen aufzubrechen und an Lösungen zu arbeiten.

Seit 2011 gehören dem LPR NRW 38 Mitglieder an. Der Großteil repräsentiert gesellschaftliche Organisationen, wie Kirche, Kommunen, Wissenschaft und Wohlfahrt, Gewerkschaften und Verbände. Zu einem kleineren Teil kommen sie aus verschiedenen Ministerien des Landes. Den Vorsitz des LPR NRW hat Staatsminister a. D. Prof. Jochen Dieckmann inne. Die Geschäftsführung liegt beim Justizministerium NRW.

Eine junge Frau genießt ihren Urlaub in Italien und postet Bilder davon auf Facebook. Plötzlich erhält einer ihrer Bekannten eine Facebook-Nachricht von ihr: »Hilf mir bitte – ich bin ausgeraubt worden! Kannst du mir bitte 600 Euro per Moneytransfer überweisen?« Der Bekannte zögert nicht lange und überweist ihr das Geld. Was beide nicht wissen: Dritte haben sich unbemerkt Zugang zu dem Facebook-Account der jungen Frau verschafft und von dort die Nachricht verschickt. Der Film »Account-Takeover« zeigt eindrücklich, wie wichtig ein vorsichtiger Umgang mit Passwörtern ist.

»Wir wollten so etwas in der Art machen, wie die Verkehrssicherheitsfilme »Der 7. Sinn«, nur eben für den Bereich Internetsicherheit. Jeder Kurzfilm behandelt dabei ein eigenes Thema und wendet sich an eine klar definierte Zielgruppe – also zum Beispiel Jugendliche, Senioren oder Unternehmen«, erklärt Peter Vahrenhorst, Mitarbeiter im Cybercrime-Kompetenzzentrum NRW. Bislang wurden 16 Kurzfilme entwickelt, die Themen reichen von Cybermobbing, Account-Übernahme und Datenklau über E-Mail-Sicherheit bis hin zu Online-Banking oder Smartphone-Apps. »In den Filmen wird jeweils ein Risiko aus dem Bereich Cybercrime beschrieben und Hilfestellung dazu gegeben. Es wird jedoch bewusst keine komplette Problemlösung angeboten, da wir die Menschen zum Nachdenken anregen wollen. Es geht darum, ein Risikobewusstsein zu schaffen«, betont der Experte. Einige der vorgestellten Themen werden in den Filmen auch aus verschiedenen Blickwinkeln betrachtet, so gibt es zum Phänomen Cybermobbing etwa Kurzfilme aus der Perspektive des Opfers, des Täters oder auch des Umfelds. Vahrenhorst: »Wichtig ist neben der Identifizierung eines Themas die Festlegung der Zielgruppe. An wen soll sich der Film richten? Senioren muss ich anders ansprechen als Jugendliche und die Inhalte müssen jeweils anders aufbereitet werden.« Der Weg von der Idee bis zum fertigen Film ist kurz, so dass auch relativ schnell auf neue Phänomene reagiert werden könnte. »Ein Gremium legt zunächst >



Thema und Zielgruppe fest, dann wird zusammen mit einem externen Regisseur und einem Kamerateam ein Filmkonzept entwickelt. Im günstigsten Fall dauert es bis zum fertigen Film nur rund vier Wochen.«

Positives Feedback – auch aus dem Ausland

Die Filme werden nicht nur in der polizeilichen Prävention eingesetzt, sondern auch in Schulen oder in anderen Einrichtungen gezeigt, die im präventiven Bereich tätig sind. »Es gab auch Anfragen von der Schweizer Polizei, die die Filme sogar ins Italienische und Französische übersetzen lassen will. Auch Unternehmen nutzen die Filme für interne Schulungen«, freut sich Peter Vahrenhorst über das allgemein positive Feedback. Zusätzlich zu den Filmen wird auch Begleitmaterial zur Verfügung gestellt, welches zum Beispiel Hintergrundinformationen zu den jeweiligen Themen enthält, damit die Durchführenden auch weitergehende Fragen zu den Cybercrime-Phänomenen beantworten können. »Von den Kolleginnen und Kollegen aus der Seniorenprävention kann man zum Beispiel nicht unbedingt erwarten, dass sie sich gut mit dem Thema Cybercrime auskennen. Ein Leitfaden unterstützt sie, wenn sie einen der Filme in ihrer Arbeit einsetzen möchten.«

Das Gremium des Landespräventionsrats ist ständig auf der Suche nach weiteren Cybercrime-Themen, die man filmisch umsetzen kann. Auf der Internetseite www.sichere-netzwelten.de werden alle Filme zum freien Download angeboten. ///

Simone Wroblewski

NRW-PRÄVENTIONSPROJEKT »BISTAND«

Der Begriff »Bistand« stammt aus dem Plattdeutschen und bedeutet »Helfer« oder »Beschützer«. Bei der Kampagne »Bistand« des Gremiums »Sicherheit in Rheine« (SIR) geht es um das Thema Cybermobbing, Zielgruppe sind Schülerinnen und Schüler der Jahrgangsstufen fünf bis zehn. Auch die Kreispolizeibehörde Steinfurt beteiligt sich an dem Projekt. Der Anlass, um die Initiative ins Leben zu rufen, war eine anonyme Umfrage unter Schülern in Rheine im Frühjahr 2012. Ihr Ergebnis: Cybermobbing ist ein Problem, auch an den Schulen in Rheine. Nach den Sommerferien 2012 wurde im Rahmen des Projekts daher an allen weiterführenden Schulen in Rheine ein Informations- und Medienpaket verteilt, um das Thema im Unterricht zu behandeln. Am Ende der erfolgreichen Teilnahme am Unterricht geben sie eine Selbstverpflichtungserklärung zum verantwortungsvollen Umgang mit dem Internet ab und erhalten eine Bescheinigung in Form einer Scheckkarte. Es ist geplant, in einer erneuten Umfrage zu überprüfen, ob die Kampagne erfolgreich ist.

NRW-PRÄVENTIONSPROJEKT »S.I.N.U.S – SICHER IM NETZ UNTERWEGS«

Das regionale Netzwerk »s.i.n.us – Sicher im Netz unterwegs« ist ein Zusammenschluss von Institutionen aus den Bereichen Schule, Eltern, Jugend- und Suchthilfe und der Kreispolizeibehörde Rhein-Kreis Neuss. Das Projekt fördert die Medienkompetenz von Schülerinnen und Schülern, Lehrerinnen und Lehrern sowie Eltern. Es informiert die jeweiligen Zielgruppen über mögliche Online-Risiken sowie den sicheren und verantwortungsbewussten Umgang mit dem Internet. Im Jahr 2014 standen bei dem Projekt die Themen Datensicherheit in Sozialen Netzwerken, sexualisierte Gewalt in den digitalen Medien, Extremismus 2.0 und Online-Sucht im Fokus. Durch s.i.n.us kann das breite Spektrum von Cybercrime umfassend in eigenen Veranstaltungen dargestellt werden. Ein Themenschwerpunkt der Kreispolizeibehörde Rhein-Kreis Neuss ist die Datensicherheit in Sozialen Netzwerken.

Weitere Informationen zu s.i.n.u.s erhalten Sie unter:
www.schulentwicklung.nrw.de/sinus

PRÄVENTIONS-TIPP

SICHERE PASSWÖRTER

> Ein sichereres Passwort hat mindestens acht Zeichen, kommt nicht im Wörterbuch vor und besteht aus einer Kombination von Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen. Tipp: Man denkt sich einen Satz aus, den man leicht behalten kann und verwendet die Anfangsbuchstaben der darin vorkommenden Wörter (Klein- und Großschreibung unterscheiden) sowie die Sonderzeichen inkl. Satzzeichen. Beispiel: Ich fahre nach der Arbeit gerne 3mal pro Woche zum Sport. = IfndAg3pWzS.$
> Vermeiden Sie triviale Passwörter wie »geheim«, »ABC1234« oder bloße Tastaturmuster wie etwa »asdfgh« oder »67890ß«.
> Verwenden Sie insbesondere für verschiedene Anwendungen im Internet z. B. Login für E-Mail, Online-Banking, Online-Shopping jeweils unterschiedliche Passwörter.
> Ändern Sie immer voreingestellte Passwörter, unabhängig von der Anwendung/Hardware.
> Wenn Sie Passwörter notieren, dann sicher und getrennt vom PC.

Ein Video des Landespräventionsrats NRW zeigt, was beim Passwort-Phishing geschieht.

SCHUTZ VOR PHISHING

> Vermeiden Sie, auf Links in zugesandten E-Mails zu klicken. Dies gilt in besonderem Maß für E-Mails, die unaufgefordert geschickt wurden.
> Seien Sie misstrauisch, wenn Sie aufgefordert werden, vertrauliche Daten preiszugeben. Kreditinstitute werden Sie niemals per E-Mail, per Telefon oder per Post dazu auffordern. Halten Sie im Zweifelsfall Rücksprache mit Ihrer Bank.
> Machen Sie sich mit dem gewohnten Ablauf bei Transaktionsvorgängen innerhalb Ihrer Online-Banking-Anwendung vertraut. Seien Sie misstrauisch bei Änderungen innerhalb der Abläufe, brechen Sie im Zweifelsfall die geplanten Transaktionen ab.
> PIN und TANs sollten Sie nur bei einer gesicherten Verbindung über Ihren Browser eingeben, erkennbar daran, dass die Adresszeile mit »https://« beginnt.
> Stellen Sie bei Nutzung externer Zugangssoftware für das Online-Banking sicher, dass es sich um die offizielle Softwareversion Ihrer Bank handelt.

Das Video »E-Mail-Sicherheit« des Landespräventionsrats NRW zeigt, worauf man bei E-Mails achten muss.

Die Videos des Landespräventionsrats NRW zu diesen Tipps finden Sie im Internet unter: www.sichere-netzwelten.de

GLOSSE

Einen Medienscout, bitte!

Meine Freundin konnte früher schlecht rechnen. Folglich bekam sie damals Nachhilfeunterricht in Mathe vom pickeligen Nachbarsjungen. Ihre Tochter, mittlerweile im zweiten Schuljahr, bekommt heute einen Medienscout an die Hand, damit die Kleine das Pensum von 3.000 WhatsApp-Nachrichten an einem Schultag möglichst fehlerfrei schafft. Senioren bekommen einen Medienscout von der Volkshochschule, damit sie überhaupt noch mitbekommen, dass PIN und PUK nicht die Zwillinge ihrer Enkeltochter sind.

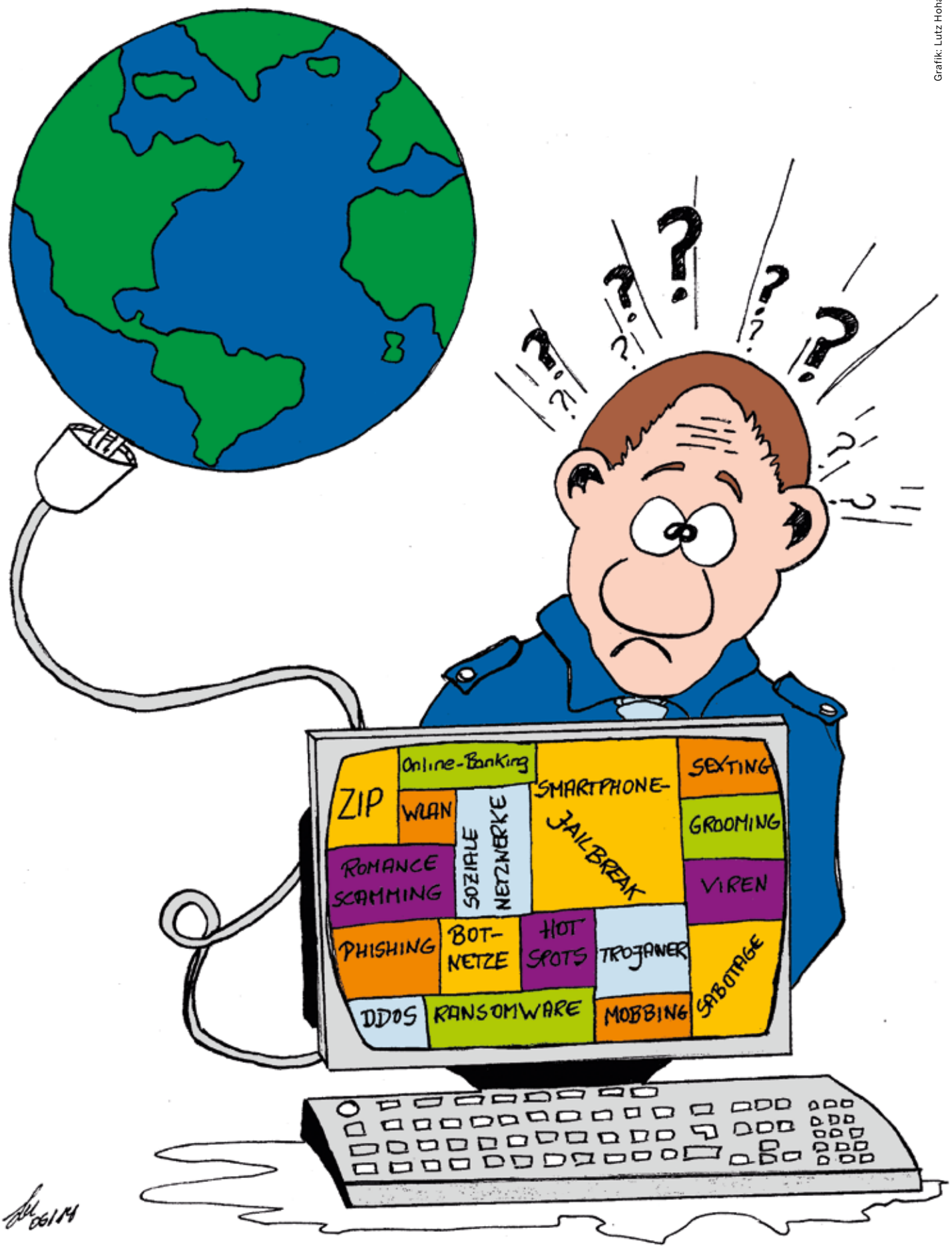
So ein Medienscout kann ja auch die Form eines Gerätes einnehmen. Moderne Kassiererinnen haben sowas jetzt. Wo sie noch früher die Summe der Waren selbst zusammenrechnen, gleichzeitig die Hand aufhalten, den Kunden freundlich anlächeln und den passenden Tagesgruß parat haben mussten, reicht heute ein verschwiegener und bestimmender Fingerzeig auf die Maschine vor ihnen, in die der Kunde gefälligst das Scheinchen hineinzuschieben hat. Tolle Sache.

Wie wäre es mit einem Medienscout für die Polizei? Nein. Nicht so ein neuer Yelp-Ton, der jedes Trommelfell in die Knie zwingt. Noch mehr großes Geheul hilft uns in diesen schweren Zeiten nicht weiter. Ich meine einen Medienscout, der uns an die Hand nimmt, bei der rasanten Verlagerung von polizeilichen Ermittlungen in die digitale Welt. Einer, der dafür sorgt, dass wir nicht auf halbem Wege in die Anonymisierung abgehängt werden.

Die schönen alten Zeiten, in denen der A dem B ganz realistisch und analog eins auf die Zwölf gehauen hat, sind vielleicht bald vorbei. Wir müssen also umdenken. Unseren Arbeitsalltag neu konfigurieren. Der »Erste Angriff« ist nicht mehr der, der er einmal war. Heute befragen wir bei der Wohnungsdurchsuchung zuerst »SIRI«, ob ihr irgendetwas Außergewöhnliches aufgefallen ist und dann erst den Nachbarn.

Wo ist unser Kassenautomat, der uns den Umgang mit dem TOR-Netzwerk, den Distributed Denials Of Services oder der Ransomware erleichtert? Wo ist unser pickeliger Nachbarsjunge, der versucht, uns die binomischen Formeln der Cybercrime und die damit verbundenen Entwicklungen in der Polizeiarbeit zu erklären? Was rate ich der Tochter meiner Freundin eines Tages, wie sie die Nacktbilder ihres übergewichtigen Leibes wieder aus einer der 5.350.000 WhatsApp-Nachrichten herausbekommt? Einen Medienscout bitte, schnell! ///

Claudia Franken, LKA NRW



Grafik: Lutz Hohaus, LKA NRW

Knotenpunkt polizeilicher Daten:
Andreas Lezgus in einem Serverraum des LZPD

Foto: Jochen Tack

Angriffe aus dem Netz

»Wir tun alles, um Polizeidaten zu schützen«

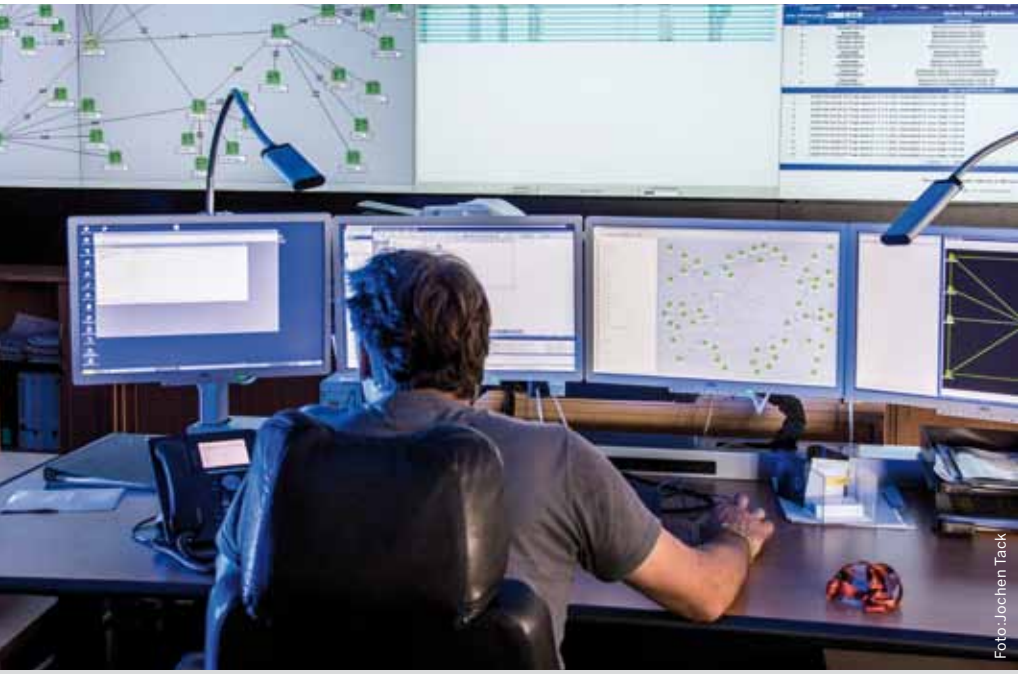
Nicht nur Wirtschaftsunternehmen stehen im Fokus von Cyberkriminellen. Auch öffentliche Einrichtungen und Behörden wie die Polizei sind ein beliebtes Ziel – sie müssen mit täglichen Attacken aus dem Netz rechnen. Die Polizei NRW ergreift daher komplexe Maßnahmen, um die Polizeibehörden und ihre rund 50.000 Mitarbeiterinnen und Mitarbeiter vor Angriffen zu schützen.

Angriffsszenarien gibt es viele: Von sogenannten Distributed-Denial-of-Service-Attacken, zum Beispiel auf einen zentralen Dienst der Polizei, wie etwa den Internetauftritt oder das Bewerberportal bis zu einer Vielzahl an Angriffstechniken auf interne Datenbestände. »Bei diesen DDoS-Angriffen senden Cyberkriminelle gezielt massenhaft Anfragen an unsere Server, so dass der jeweilige Dienst für andere nicht mehr zu erreichen wäre, wenn nicht rechtzeitig darauf reagiert würde«, erklärt der Leitende Polizeidirektor Andreas Lezgus vom Landesamt für Zentrale Polizeiliche Dienste (LZPD) NRW in Duisburg. »Solche Angriffe versuchen wir in der Regel aber frühzeitig zu erkennen und leiten dann die ankommenden Datenströme um, so dass die betroffenen Dienste auch weiterhin erreichbar sind.« Ansonsten sei es hauptsächlich Schadsoftware in E-Mail-Anhängen oder auf Webseiten, mit denen Cyberkriminelle versuchten, Zugriff zu internen Systemen und Datenbeständen zu erlangen. »Diese Art von Angriffen werden durch unsere Sicherheitswerkzeuge gefiltert. Sie prallen quasi schon an der Außenhaut ab«, erklärt Lezgus.

Ein umfangreiches, mehrstufiges Informationssicherheits-Konzept sorgt dafür, dass Cyberkriminelle es möglichst schwer haben, erfolgreich einen Angriff durchzuführen. Grundlage des Konzeptes sind die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI), die im »IT-Grundschutz« des BSI festgehalten sind. Darin sind Datenbestände etwa nach bestimmten Kategorisierungen gruppiert: Je kritischer und vertraulicher die zu schützenden Daten sind und je nachdem, wie verfügbar die Daten sein müssen, desto höhere Schutzempfehlungen gibt es. »Wir tun eine Menge, um Polizeidaten zu schützen. Die Polizei arbeitet mit sehr sensiblen Datenbeständen, die einen hohen Schutzbedarf haben, wie etwa Fahndungsdaten, allgemeine polizeiliche Vorgangsdaten oder auch der Austausch mit Staatsanwaltschaften. Daher benötigen wir sehr hohe Sicherheitsstandards, die wir mit unseren verschiedenen Maßnahmenpaketen auch erfüllen«, erklärt der Experte. Die BSI-Maßnahmen beziehen sich zum Beispiel auf die Themen »Gefährdungen«, wie etwa »technisches Versagen«, »menschliche Fehlhandlungen« oder »organisatorische Mängel« sowie unter anderem auf die Bereiche »Infrastruktur«, »Personal«, »Hardware- und Software« oder »Kommunikation«. »Werden alle empfohlenen Maßnahmen des BSI umgesetzt, erreicht man ein hohes Sicherheitsniveau – so auch die Polizei NRW.«

Geprüfter Software-Mix sorgt für Sicherheit

Die Polizei NRW arbeitet mit Produkten verschiedenener Hersteller, etwa von Antivirensoftware, Sicherheitsgateways oder zur Verschlüsselung von Systemen. Interne Sicherheitsbeauftragte prüfen bei Ausschreibungen für diese Produkte, ob die strengen Sicherheitsstandards eingehalten werden. Es wird aber auch eigene Software entwickelt, die neben internen Prüfmaßnahmen zudem von externen Firmen, die auf solche Sicherheitsanalysen spezialisiert sind, getestet wird. Diese Unternehmen führen so genannte Penetrationstests durch, das heißt, sie testen die entwickelte Software auf bereits bekannte, aber auch auf neue Sicherheitslücken. Dabei arbeitet die Polizei unter anderem auch mit Universitäten zusammen, so dass dabei auch die neusten Forschungserkenntnisse einfließen können. Externe Auditoren prüfen außerdem unter anderem die Schnittstellen zu den anderen Polizeien der Länder und des Bundes, um >



Die IT-Leitstelle – Ein 24-Stunden-IT-Service für eine professionelle Polizei

die Sicherheit der Polizeinetzstrukturen zu gewährleisten. »In diesen Audits prüft die Polizei mit wechselnden Sicherheitsexperten, ob und wie die Sicherheitsmaßnahmen des BSI umgesetzt wurden und inwiefern sie bundesweit einheitlich beziehungsweise vergleichbar sind«, so der Leitende Polizeidirektor.

Unterstützung durch CERTs

Als große Behörde benötigt die Polizei NRW auch die Unterstützung der führenden IT-Hersteller und arbeitet eng mit diesen zusammen. Innerhalb der IT-Unternehmen unterstützen die »Computer Emergency Response Teams« (CERTs) Kunden, die spezielle Service- und Wartungsverträge haben und informieren sie frühzeitig über neue Angriffsziele und Sicherheitsprobleme. »Große Organisationen wie wir mit bis zu 40.000 PCs benötigen bei der Beseitigung von Sicherheitslücken ausreichend Vorlaufzeit. Daher erfahren wir von entdeckten Schwachstellen häufig schon vor deren Veröffentlichung, damit wir rechtzeitig entsprechende Gegenmaßnahmen treffen können«, erklärt Lezgus. Dies sei besonders im Hinblick auf so genannte »Zero Day Attacken« wichtig, bei denen Sicherheitslücken bereits am gleichen Tag, an dem sie öffentlich bekannt werden, von Cyberkriminellen ausgenutzt werden. Neben dem Sicherheitsnetzwerk mit den IT-Herstellern ist die Polizei NRW auch mit CERTs aus Bund und Ländern eng vernetzt und tauscht sich über relevante Sicherheitsprobleme aus. »Werden Sicherheitslücken übergreifend eingesetzt, wissen wir das in der Regel ebenfalls ein paar Tage vorher, bevor in den Medien darüber berichtet wird. So können wir gemeinsam abschätzen, welche Auswirkungen eine Schwachstelle auf unsere Systeme haben könnte und welche Vorsichtsmaßnahmen getroffen werden müssen.«

Sicherheit in den Polizeibehörden

Das LZPD ist für die Sicherheit aller zentralen IT-Dienste zuständig, die von allen Polizeibehörden gemeinsam genutzt werden, zum Beispiel für das Rechenzentrum sowie für alle kritischen polizeilichen Verfahren. Für die Netzübergänge zu anderen Behörden sowie das lokale Netzwerk sind die einzelnen Polizeibehörden selbst verantwortlich, das heißt, sie müssen hier den Maßnahmenkatalog des BSI eigenständig umsetzen. Auch hier wird in regelmäßigen Audits geprüft, ob die Behörden sich an die Vorgaben halten. Will eine Behörde ein Verfahren oder eine bestimmte Software »außer der Reihe« einsetzen, muss dafür ein eigenes Sicherheitskonzept zur Genehmigung vorgelegt werden. »Wird das Verfahren genehmigt, ist die Behörde im Anschluss für eine regelmäßige Sicherheitsanalyse verantwortlich und muss sich dazu an festgelegte Sicherheitsleitlinien halten«, erklärt Andreas Lezgus.

Herausforderung Personalentwicklung

Die technischen Fortschritte im Bereich Informationstechnologie sind rasant – und benötigen hochqualifizierte Fachleute, die mit ihrem Wissen stets auf dem aktuellen Stand sind. »Die Polizei kämpft hier mit dem gleichen Problem wie alle öffentlichen Verwaltungen. Wir stehen im Wettbewerb mit den großen Softwareunternehmen, die nicht nur höhere Gehälter zahlen können, sondern auch andere Einstellungskriterien haben«, erklärt der Leitende Polizeidirektor. Um bei der Polizei im IT-Bereich einsteigen zu können, benötigt man in der Regel ein Fach- oder Hochschulstudium. Viele Experten, die im Bereich IT sehr fit sind, haben aber keines. »Die Wirtschaftsunternehmen können regelmäßig besser zahlen und sind in der Einstellungspraxis flexibler – das ist für uns problematisch«, meint der Experte. Dies kann zukünftig dazu führen, dass öffentliche Verwaltungen

wie die Polizei zunehmend prüfen müssen, ob sogenannte »gemanagte Sicherheitsbausteine« auch von externen Dienstleistern übernommen werden können. Der automatisierte und standardisierte Dienst wie etwa das Einspielen von Sicherheitspatches wird dann nach Vorgaben und Prüfungen der Polizei von externen Anbietern übernommen. »Dies wird nicht in allen Bereichen möglich sein. In besonders sensiblen Segmenten müssen wir als Polizei natürlich die Hoheit behalten und eine besondere Personalentwicklung fördern«, betont Lezgus.

Bewusstsein in den Behörden schaffen

Die geprüfte Sicherheit von Systemen ist nur ein wichtiger Baustein, wenn es um den Bereich IT-Sicherheit geht. »Fast genauso wichtig ist es, bei den Kolleginnen und Kollegen ein Bewusstsein für die Gefahren zu schaffen, die das Internet mit sich bringt«, betont der Experte. »Man muss als PC-Nutzer und Nutzer von mobilen Geräten wissen, auf welche Weise Schadsoftware verbreitet wird und dass Betrüger zum Teil sehr geschickt vorgehen, wenn es darum geht, an sensible Daten zu gelangen – das gilt privat genauso wie am Arbeitsplatz.« In den Behörden gebe es zwar höhere Filtermechanismen, die in der Regel zum Beispiel potenziell gefährliche E-Mails herausfiltern, dennoch müsse auch der Nutzer mitdenken und dürfe nicht vorschnell handeln. »Es hat auch seine Gründe, dass bestimmte Webseiten von den Behördenrechnern aus nicht aufgerufen werden können. Das soll keine Bevormundung sein, sondern dient dem Schutz der polizeilichen Daten und nicht zuletzt auch dem Schutz der Kolleginnen und Kollegen«, erklärt Andreas Lezgus. ///

Simone Wroblewski

PRÄVENTIONS-TIPP

SICHERE NUTZUNG VON ÖFFENTLICHEN HOTSPOTS

> Schalten Sie die WLAN-Funktion nur ein, wenn Sie sie auch benötigen.
> Rufen Sie am besten keine vertraulichen/sensiblen Daten über ein fremdes WLAN ab.
> Verwenden Sie – soweit möglich – gesicherte Verbindungen (z. B. https) oder ein VPN (Virtual Private Network).
> Achten sie darauf, welche Dateien bzw. Verzeichnisse Sie auf Ihrem Endgerät freigegeben haben.

SICHERES WLAN

> Schützen Sie den Administrationsbereich Ihres Routers mit einem sicheren Kennwort. Achtung: Hier sollte der Sicherheitslevel noch höher sein (20-stelliges Kennwort).
> Verwenden sie die WPA2-Verschlüsselung, nicht die relativ leicht zu überwindende WEP-Verschlüsselung.

Die Videos des Landespräventionsrats NRW zu diesen Tipps finden Sie im Internet unter: www.sichere-netzwelten.de

@ Mehr Infos zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik gibt es auf der BSI-Webseite: https://www.bsi.bund.de

Optische Tarnkappen und intelligente Kochtöpfe

Zukünftige Entwicklungen im Cyberbereich

Die größte Herausforderung wird eine Erhöhung der IT-Sicherheit sein. Doch auch andere Entwicklungen wie »Smart Home« könnten die Polizei bald stärker beschäftigen.

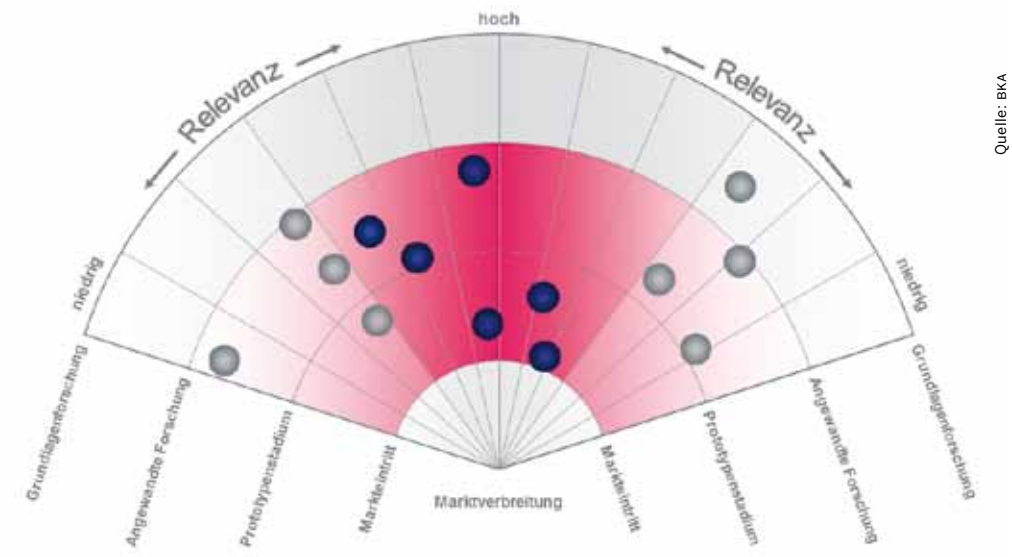
Ein Knopfdruck und das gesamte Auto wird unsichtbar. 2002 konnte James Bond in dem Film »Stirb an einem anderen Tag« mit Hilfe eines Sportwagens, der sich der Umgebung so gut anpasste, dass er für das bloße Auge unsichtbar wurde, gleich zwei Gegenspieler ausschalten. Was 2002 außerhalb eines Films noch völlig undenkbar war, ist 2015 zumindest für die ferne Zukunft nicht mehr auszuschließen. Der Grund ist die Entwicklung von optischen Tarnkappen. »Sogenannte Metamaterialien können Lichtwellen umlenken und somit zumindest kleinste Gegenstände im Labor unsichtbar machen«, erläutert Bernhard Schneider, stellvertretender Leiter der Fachgruppe »Technisches Entwicklungs- und Servicezentrum, Innovative Technologien« (TESIT) des Kriminalistischen Institutes beim Bundeskriminalamt (BKA). Diese mögliche technische Entwicklung liegt zwar auf dem regelmäßig vom TESIT herausgegebenen Technologieradar noch in sehr weiter Entfernung, doch sie hat es immerhin bis auf diesen Radar geschafft. »Dabei sprechen wir von einer Entwicklung, die noch komplett in den Kinderschuhen steckt und wohl eher 20 Jahre und mehr brauchen wird, um die Polizei zu beschäftigen«, erklärt der Diplom-Physiker. »Die Missbrauchsmöglichkeiten dieser Technologie wären aber natürlich enorm.«

Der Technologieradar bildet neue technologische Entwicklungen ab, die in Zukunft für die Polizei relevant sein könnten. Dabei haben die BKA-Mitarbeiter in etwa die kommenden drei bis acht Jahre im Blick. Der Technologieradar sieht tatsächlich aus wie ein Radarbild. Dabei steht jeder der dort abgebildeten Punkte für eine zukünftige Technologie. Je näher der Punkt am Zentrum ist, desto früher kommt diese Herausforderung auf die Polizei zu. Wie relevant diese kommende Entwicklung für die Polizeiarbeit sein wird, zeigt die Position des Punktes in der Horizontalen an. Umso weiter rechts oder links der Punkt von der Flugrichtung entfernt liegt, umso höher die Wahrscheinlichkeit, dass sich diese Technologie zwar entwickelt, aber ohne einen hohen Einfluss auf die Polizeiarbeit zu haben. »Umso weiter wir in die Ferne blicken, umso unschärfer wird dabei das Bild. Die optischen Tarnkappen liegen am äußeren Rand der Scheibe, allerdings direkt in Flugrichtung«, erklärt Bernhard Schneider.

DER TÄTER DER ZUKUNFT HINTERLÄSST KEINEN FINGERABDRUCK, SONDERN SEINE IP-ADRESSE

Smart Grid – Nutzen und Gefahren

Eine der Technologien, die seiner Meinung nach aber direkt vor der Tür steht, sind intelligente Stromnetze, auch Smart Grid genannt. Sie sollen helfen, erneuerbare Energien besser in das Stromnetz zu integrieren, indem sie durch die Installation von intelligenten Zählern die Höhe und Dauer des Verbrauchs messen und direkt an den Stromlieferer melden. Dazu werden die herkömmlichen Stromzähler durch intelligente kleine Computer ersetzt, die einen kontinuierlichen Überblick über den Verbrauch



Quelle: BKA

Der Technologieradar bildet neue technologische Entwicklungen ab, die in Zukunft für die Polizei relevant sein könnten.

SMART HOME: DIE INTELLIGENTE HAUSTECHNIK

Ein vernetzter Schnellkochtopf, der auf dem Handy Bescheid sagt, wenn die Temperatur geändert werden soll oder die nächste Zutat für das Rezept fällig ist, ist nur eine der neuen Entwicklungen aus dem Bereich »Smart Home«, die Alltagsgegenstände miteinander vernetzen und über eine Hauszentrale steuerbar machen. »Ein Autoschlüssel, der gleichzeitig auch mein Hausschlüssel ist und automatisch die Alarmanlage ausschaltet, wenn ich nach Hause komme, erleichtert das Leben«, erklärt Peter Vahrenhorst vom Cybercrime-Kompetenzzentrum. »Dieser Autoschlüssel in den falschen Händen kann aber fatal werden.« Smart Home ist ein schnell wachsender Markt. Viele Neubauten, die heute in Deutschland entstehen, haben schon Smart-Home-Elemente, wie etwa die zentrale Steuerbarkeit der Heizung über das Smartphone. »Das potenzielle Problem dabei ist, dass derjenige, der die Hauszentrale in der Hand hat, der »Hausherr« ist und das kann ganz schnell jemand anders als der Eigentümer sein«, erklärt der 51-Jährige, der sich bereits seit über 15 Jahren mit Cybercrime beschäftigt.

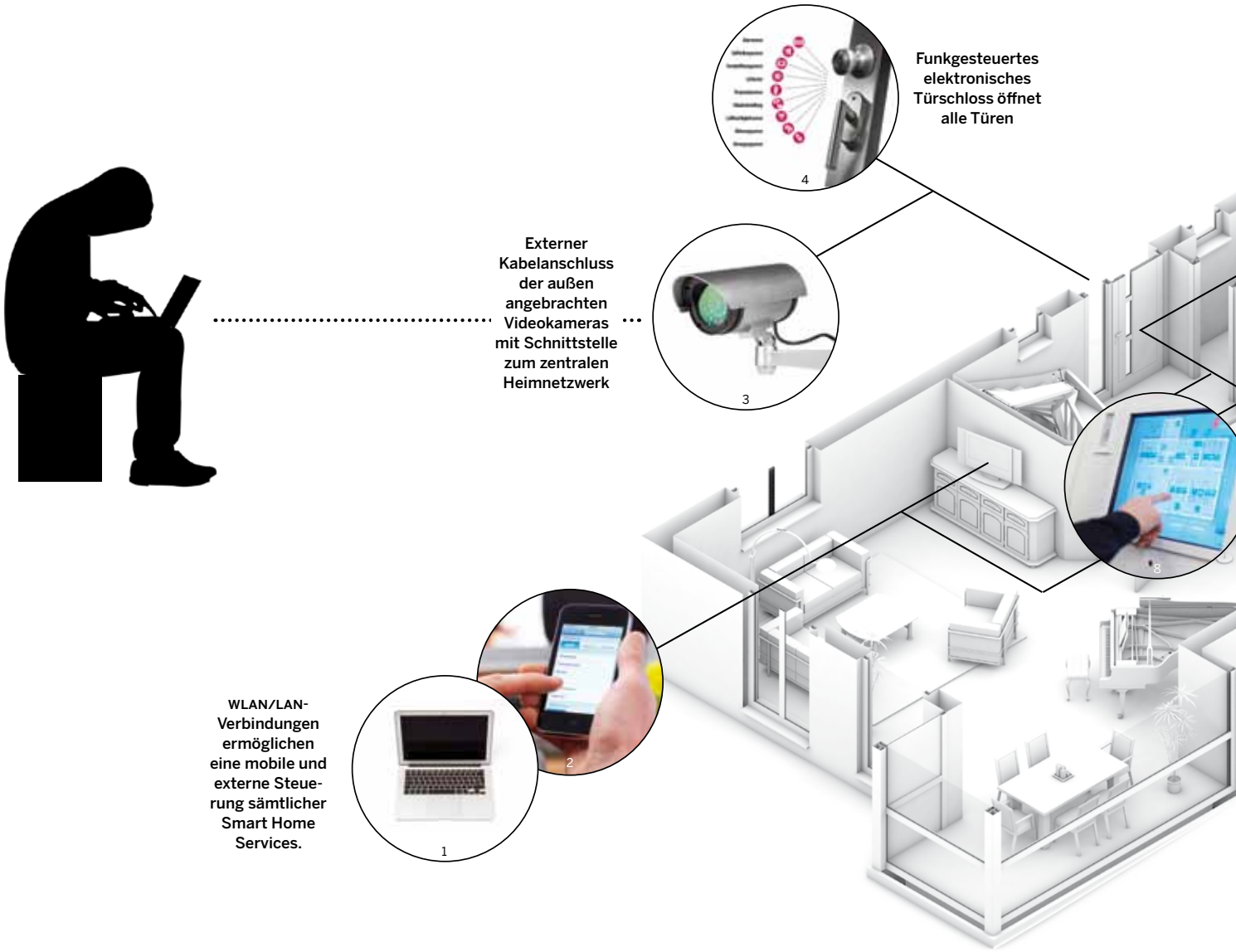
Konkrete Fälle oder Zahlen gibt es zu diesem Bedrohungsszenario zwar noch nicht, doch das Risiko ist da. Das Landeskriminalamt NRW versucht zusammen mit der VdS Schadenverhütung GmbH und der Smart Home Initiative Deutschland e. V. solchen Missbrauch zu verhindern, noch bevor er entsteht. »Das ist Neuland für uns«, sagt Peter Vahrenhorst, der seit über sechs Jahren in der Prävention von Cybercrime tätig ist. »Wir versuchen nun quasi vor die Lage zu kommen und durch das Einbringen unserer Kenntnisse Sicherheitsstandards zu schaffen, die einen Missbrauch verhindern oder zumindest einschränken können. Daher haben wir auch externen Sachverstand hinzugezogen. VdS ist ein akkreditiertes Prüf- und Zertifizierungsinstitut für Sicherheitstechnik. Die Smart Home Initiative ist ein gemeinnütziger Verein, der eine Brücke zwischen den einzelnen Beteiligten wie Herstellern, Handwerkern und Vertrieben herstellen will.«

melden können. Diese neue Entwicklung kann die Polizei einerseits für sich nutzen – andererseits kann sie aber auch das Tor für neue Missbräuche öffnen. »Die Polizei könnte anhand des Stromverbrauchs zum Beispiel feststellen, ob jemand gerade zu Hause ist oder zu einem bestimmten Zeitpunkt zu Hause war«, erläutert der BKA-Mann den möglichen Nutzen. Andererseits könnten natürlich auch Hacker sich genau dieser Daten bemächtigen und sie etwa nutzen, um in das Haus einzubrechen, wenn es gerade leer steht. Sie könnten aber auch den Strom abstellen, was vor allem bei Unternehmen zu einem gefährlichen Druckmittel für Erpressungen werden könnte.

Das intelligente Haus

Stark mit diesem Thema verwandt ist die intelligente Ausstattung des gesamten Hauses, auch bekannt unter dem Begriff Smart Home. Ein Trend, der bereits Realität wird. »Je mehr Daten digital werden, desto höher ist auch die Gefahr des Missbrauchs«, betont Bernhard Schneider. Er geht davon aus, dass der elementare Einfluss der Informationstechnik auf das alltägliche Leben in Zukunft noch stark zunehmen wird, so dass es spätestens in zehn Jahren ohne Internet wohl nicht mehr möglich sein wird, am gesellschaftlichen Leben teilzunehmen, geschweige denn seinen Alltag zu meistern. >

IST EIN »DIGITALER« EINBRUCH IN EIN EINFAMILIENHAUS ZUKÜNFTIG MÖGLICH?



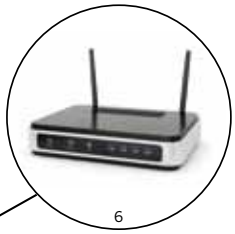
Um die Gefahren der Cybercrime einzudämmen setzt der Diplom-Physiker vor allem auf eine Erhöhung der IT-Sicherheit. »Als das Internet in den 1960er Jahren entwickelt wurde, war niemandem bewusst, wie es heute genutzt wird. Daher erfüllen die damals entwickelten Protokolle, die auch heute noch genutzt werden, nicht die wesentlichen Sicherheitsanforderungen«, erläutert er. »Da die IT-Sicherheit aber viel Geld kostet und kaum Gewinne abwirft, wird sie zurzeit noch sehr stiefmütterlich behandelt.«

Die Sicherheit als Dreh- und Angelpunkt

Ähnlich sieht das Prof. Norbert Pohlmann, geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälischen Hochschule. Die mangelnde Sicherheit in der Informationstechnik ist für ihn das Problem Nummer eins: »Unsere Software ist einfach nicht sicher. Die zahlreichen Fehler, die vorhanden sind, sind für die Angreifer eine willkommene Schwachstelle, die sie gerne nutzen.« Er geht davon aus, dass mindestens auf jedem fünfzehnten Computer in Deutschland Schadprogramme, intelligente Malware, vorhanden ist. Viele Nutzer hätten nach wie vor nicht die richtige Kompetenz, um im Netz zu surfen. Hier müsste noch viel Aufklärungsarbeit geleistet werden. »Rund 30 Prozent der Internet-Nutzer besitzen keine Firewall und 28 Prozent haben keine Anti-Malware-Produkte auf dem Rechner. Selbst bei Computern, bei denen die Nutzer der Meinung sind, dass sie optimal gesichert sind, weil sie ein Virenschutzprogramm benutzen, liegt die Wahrscheinlichkeit, dass ein Angriff auf Anhieb klappt, immer noch bei 27 Prozent«, berichtet der Gründer des Instituts für Internet-Sicherheit. »Wenn jemand beliebig viel Zeit hat und sich in der Materie auskennt, kann er sowieso jeden Computer knacken.«

Das Institut testet regelmäßig, wie viele Websites von Schadprogrammen befallen sind. Deutschland schneidet dabei nicht besonders gut ab. Während 2,5 Prozent aller in Deutschland gemessenen Websites ein Schadprogramm enthalten, sind es in

5



6

7

Zentrale Steuerung des Netzwerks vom Heimrechner regelt das gesamte Smart Home

Heizungsanlagen in Verbindung mit funkgesteuerter Lüftung oder funkgesteuerten Fenstern können auch mit Apps und Smartphones von unterwegs gesteuert werden.

NRW-Landeskriminaldirektor Dieter Schürmann hierzu:

Die Welt wird in Zukunft noch digitaler als sie es heute schon ist. Durch das »Internet der Dinge« könnte bald jedes Fahrzeug, aber auch jede Wohnung und jedes Haus samt Kühlschrank, Fernseher und Türschloss digital steuerbar sein. Das bietet einerseits mehr Komfort und viele ökologische sowie ökonomische Vorteile. Gleichzeitig muss man aber auch die Risiken dieser Entwicklungen sehen, denn auch Kriminelle nutzen diese Techniken für ihre Zwecke. Somit werden analoge Formen der Tatbegehung immer mehr zu digitalen – die von der Polizei aber auch als solche erkannt werden müssen.

Japan zum Beispiel nur 0,57 Prozent. Auch er sieht die Aufgabe bei den großen Unternehmen, die nach wie vor zu wenig Geld für IT-Sicherheit ausgeben und häufig auch kein ausreichendes Problembewusstsein haben. Natürlich könne man seine Firmen-Mails in der Bahn auf dem eigenen Handy lesen, doch dann können das im Zweifelsfall der Sitznachbar und ein Hacker auch. Die zentrale Frage lautet: Handelt es sich dabei um Daten, die schützenswert sind oder nur um die Terminfindung für den nächsten Teamausflug. >

Komfortables Bedienen und Steuern
durch eine anschauliche Visualisierung der Wohnräume

Foto: BAB

Das Problem der nationalen Alleingänge

Einige Sicherheitsprobleme bestehen schon seit langer Zeit. So ist etwa die nach wie vor vorherrschende Identifikationsmöglichkeit im Internet die Kombination aus einem Benutzernamen und einem Passwort. »Diese Identifikationsmöglichkeit war noch nie sicher«, so Prof. Norbert Pohlmann. Doch sie bietet andere Vorteile, die zurzeit schwerer wiegen: Sie ist günstig und jedes Unternehmen und jeder Staat kann unabhängig voneinander agieren. Die Vorstöße einzelner Länder sind dabei problematisch. Der neue deutsche Personalausweis enthält etwa eine eID-Funktion, mit deren Hilfe man sich eindeutig im Netz identifizieren kann. »Andere Länder verfügen nicht über solche Möglichkeiten. Die eID-Funktion ist gut konzipiert und technisch umgesetzt, doch aufgrund von mangelnder Werbung hat nur rund ein Drittel der Bürger diese Funktion überhaupt aktiviert«, berichtet Prof. Norbert Pohlmann. Im internationalen Internet haben solche nationalen Ansätze kaum eine Chance, denn die großen Online-Kaufhäuser oder auch Social-Media-Plattformen kommen aus den USA.

Für eine starke Authentifizierung, die zum Beispiel mit einem Token, also einem "elektronischem Schlüssel", arbeiten würde, müssten sowohl die Länder als auch die Unternehmen stärker zusammenarbeiten. »Die Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien ist da schon ein guter Anfang, doch wir brauchen noch mehr Initiativen in diese Richtung«, so der 54-Jährige. Er fordert einen runden Tisch, an dem Anwender, IT-Sicherheitsindustrie, Regierungsvertreter und Forscher eine gemeinsame IT-Sicherheitsstrategie für Deutschland entwickeln. Obwohl ein globales Vorgehen im Internet sicherlich immer die erste Wahl ist, so ist er der Meinung, dass Deutschland in manchen Bereichen durchaus eine Vorreiterrolle übernehmen könnte, etwa bei Verschlüsselungen. »Wir haben in puncto Sicherheit einen guten Ruf und den könnte man ruhig nutzen«, erklärt er.

Zentral Verantwortung für IT-Sicherheit übernehmen

Für die Zukunft empfiehlt er einen Paradigmenwechsel. Weg von Firewalls und Antivirenschutzprogrammen, die versuchen, alle Inhalte zu schützen, hin zu einem gezielten Absichern von tatsächlich relevanten Daten. Und er wünscht sich eine zentrale Stelle, die die Verantwortung für die IT-Sicherheit übernimmt und alles aufeinander abstimmt. Diese zentrale Stelle könnten etwa nach dem Vorbild der Automobilindustrie die Hersteller sein: »Ein Automobilhersteller hat schließlich auch zig Zulieferer, aber er garantiert, dass die Einzelteile alle aufeinander abgestimmt sind und übernimmt die Verantwortung für das Gesamtprodukt«, erläutert er. Er geht so weit zu sagen, dass, wenn sich nicht etwas Wesentliches ändert, wir in fünf Jahren das Internet nicht mehr so nutzen können wie bisher. »Ich beschäftige mich seit 1984 mit dem Thema IT-Sicherheit und kann getrost sagen: Bisher ist sie jedes Jahr schlechter geworden. 1988 hätte sich noch niemand vorstellen können, dass mal Endgeräte angegriffen werden. Wir müssen langsam anfangen, besser zu werden. Von alleine wird da nichts passieren.« ///

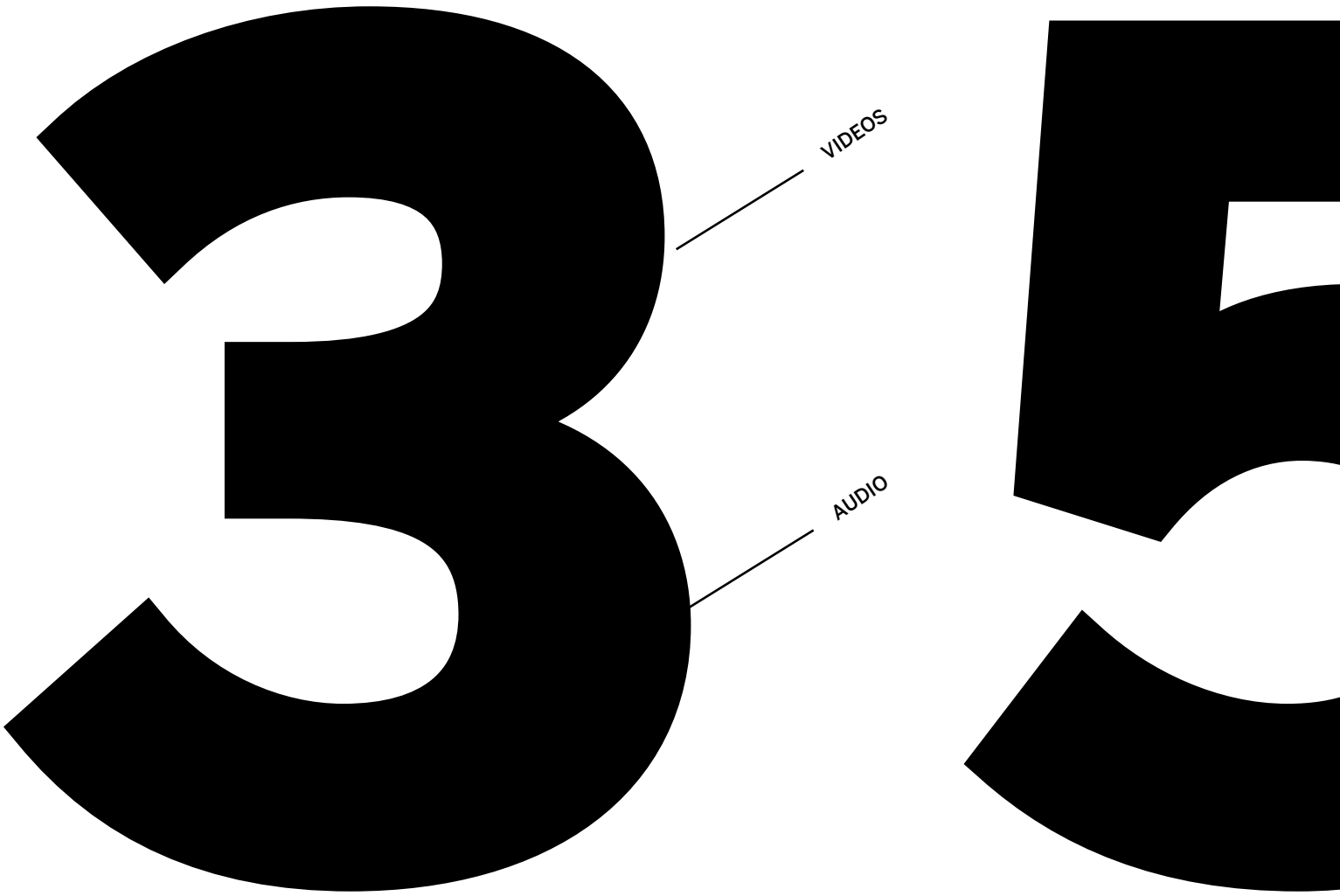
Katerina Breuer

DAS TESIT BEIM BUNDESKRIMINALAMT

Das Technische Entwicklungs- und Servicezentrum, Innovative Technologien (TESIT) existiert in dieser Form seit 2006 beim Bundeskriminalamt (BKA). Das TESIT ist zuständig für die IT-Forensik und bietet den Polizeibehörden Unterstützung bei großen Datenmengen und der operativen Einsatzunterstützung an. Wenn dabei neue Erkenntnisse gewonnen werden, von denen auch die Länder profitieren könnten, werden diese zur Verfügung gestellt.

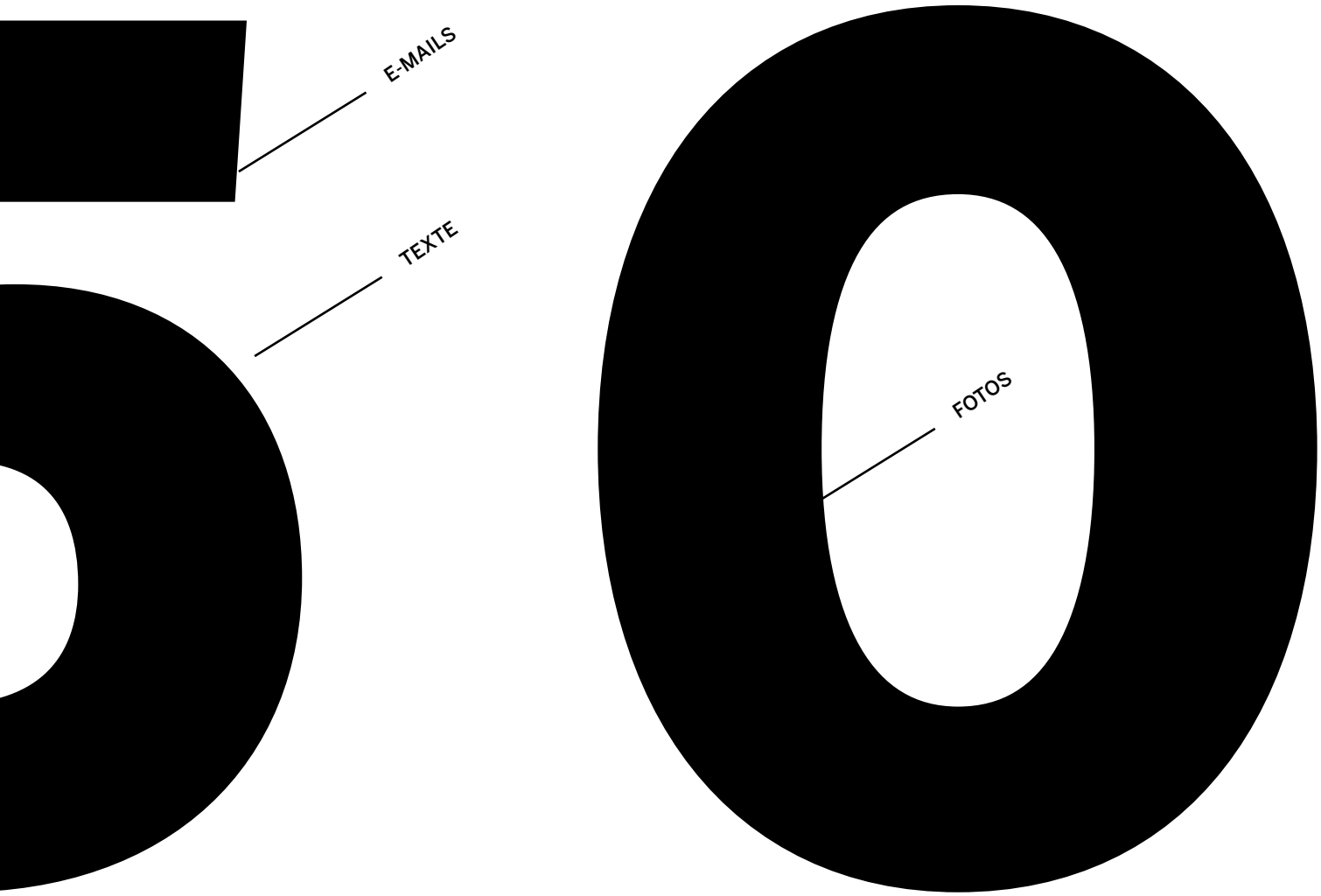
Für den Technologieradar sammeln die BKA-Mitarbeiter Informationen anhand von Veröffentlichungen und Gesprächen mit Experten in Forschungseinrichtungen. Anhand dieser identifizieren sie bis zu 200 Themen, die sie dann in Workshops mit einem Expertenkreis aus Polizeibeamten, Wissenschaftlern und Kriminologen auf die 20 bis 30 relevanten Themen eingrenzen, die schließlich auf dem Radar abgebildet werden. Als 2001 der erste Technologieradar erschien, waren darauf schon die großen Trends erkennbar, die auch heute noch aktuell sind, wie etwa die starke mobile Nutzung des Internets. Im Laufe des Jahres 2015 soll der neue Technologieradar erscheinen. Hierzu werden immer Interessierte gesucht, die sich mit ihrer fachlichen Expertise in die Themenidentifizierung und Bewertung einbringen möchten. Kontakt: KI21@bka.bund.de.

@ Das TESIT finden Sie im Internet unter: www.bka.de



»Big Data« Die Polizei im Kampf gegen die Datenflut

E-Mails, Fotos, Videos, Telefongespräche, Chats – die Polizei muss im Rahmen ihrer Ermittlungsaufgaben eine schier unüberschaubare Menge an Daten auswerten. Und die Datenflut wird immer größer und komplexer. Nicht nur die Speicherung der enormen Datenmengen stellt die Behörden vor große Herausforderungen, sondern auch die Decodierung der verschiedenen Datenformate.



BYTE

Unter dem Stichwort »Big Data«, also »große Datenmengen«, lassen sich hauptsächlich drei Problemfelder zusammenfassen, die auch die Polizei in Zukunft beschäftigen werden. Der erste Bereich ist die tatsächliche Menge der Daten, die mit den fortschreitenden technischen Entwicklungen und Möglichkeiten immer größer wird. »Während wir uns früher nur mit »internen« Datenbeständen, zum Beispiel auf beschlagnahmten Festplatten, befassen mussten, kommen heute zunehmend auch andere Quellen aus externen Rechenzentren oder aus öffentlich zugänglichen Quellen wie den Sozialen Medien hinzu. In Zukunft werden für uns zusätzlich auch Daten im Rahmen des »Internets der Dinge« ermittlungsrelevant, also etwa gespeicherte Daten aus tragbaren Gegenständen, die wir alltäglich nutzen. Das sind enorme Mengen, die gespeichert und analysiert werden müssen«, erklärt Helmut Picko, Leiter des Dezernates 41 des Cybercrime-Kompetenzzentrums im LKA NRW. Im Jahr 2013 wurden allein in den Ermittlungskommissionen des Cybercrime-Kompetenzzentrums 170 Terabyte an Daten analysiert. Ein Terabyte entspricht dabei 1.000 Gigabyte. »2014 haben wir bereits 350 Terabyte an zu analysierendem Datenmaterial in einem einzigen Ermittlungsverfahren erreicht« >

Als zweites stellen die vielen verschiedenen Datenformate ein weiteres Problem dar. Durch die unterschiedlichen Kommunikationsmittel nimmt auch die Vielfalt an Daten stetig zu, da die Daten in verschiedenen Formaten gespeichert werden und somit unterschiedlich decodiert werden müssen. Während es sich früher hauptsächlich um strukturierte Daten aus Datenbanken handelte, haben es die Ermittler nun mit vielen unstrukturierten Datenbeständen, zum Beispiel Audio- und Videodateien, Protokolle aus Voice-over-IP-Telefonaten oder E-Mails zu tun. »Diese enorm großen Datenströme in ihren unterschiedlichen Formaten müssen jetzt so analysiert werden, dass man die für die Ermittlung eigentlich relevanten Informationen herausfiltern kann. Und das ist sehr schwierig«, erklärt Helmut Picko.

Als dritte Herausforderung im Bereich »Big Data« gilt die Geschwindigkeit der Datenauswertung. Während es früher darum ging, wöchentliche oder tägliche Auswertungen zu machen, sind heute zunehmend stündliche, minütliche oder gar Auswertungen in Echtzeit nötig. »Wenn man erst einmal zwei oder drei Tage braucht, um bestimmte Daten auszuwerten, nimmt das Entdeckungsrisiko für die Täter ab – Geschwindigkeit und Echtzeitanalysen sind also Faktoren, die künftig immer wichtiger werden«, betont Picko.

Nicht zuletzt haben auch Bürgerinnen und Bürger eine hohe Erwartungshaltung an die Arbeit der Polizei. Ein seriöser und sicherer Umgang mit den Daten wird vorausgesetzt. »Das ist immer eine Gratwanderung. Einerseits wird erwartet, dass die Polizei umfangreiche Maßnahmen etwa im Bereich der Analyse von Kinderpornografie ergreift. Bei anderen Themen wird das durchaus kritischer gesehen – zum Beispiel, wenn es um die Verknüpfung von öffentlichen Daten geht. Dieser Bereich ist sensibel und wird daher von uns mit größter Vorsicht angegangen. Die Polizei darf nicht über das Ziel hinausschießen«, betont Helmut Picko.

Mehr Geld, mehr Speicher, mehr Experten

Um technisch auf dem aktuellen Stand zu bleiben und sich neue Technologien erschließen zu können, sind neue Investitionen notwendig. »Was wir hauptsächlich benötigen, sind Werkzeuge für Datenanalysen wie beispielsweise zur Massendatenauswertung und die Analyse von umfangreichen Videodaten – etwa im Bereich Kinderpornografie«, so Picko. Auch für die Speicherung der Daten wird für die Zukunft nach Alternativen zu den klassischen Rechenzentren gesucht, da diese schon bald keine ausreichenden Kapazitäten für die Speicherung der zunehmenden Datenmengen haben werden. Hier bieten sich externe Cloud-Lösungen an, bei denen jedoch kritisch geprüft werden muss, ob die Anbieter die strengen rechtlichen und sicherheitstechnischen Anforderungen erfüllen können, die in Deutschland gelten. »Viele internationale Cloud-Anbieter kommen für uns derzeit nicht in Frage, weil sie unsere datenschutzrechtlichen Bedingungen noch nicht einhalten können. Derzeit prüfen wir, ob wir vergleichbare Technologien länderübergreifend innerhalb der Polizeien von Bund und Ländern einsetzen und die Anforderungen gemeinsam bündeln können. Daneben arbeiten wir mit externen deutschen Anbietern zusammen, um Lösungen für die Zukunft anzubieten«, erklärt der Leitende Polizeidirektor Andreas Lezgus vom Landesamt für Zentrale Polizeiliche Dienste (LZPD) NRW. Ein weiteres Problem: Für

Foto: Jochen Tack

Helmut Picko, Leiter des Dezernates 41 des Cybercrime-Kompetenzzentrums

den Bereich Big Data sind IT-Experten nötig, die Erfahrung mit der Auswertung von großen Datenmengen haben – diese sind aber nur begrenzt auf dem Arbeitsmarkt verfügbar. Hier kämpfen aber nicht nur die Öffentlichen Verwaltungen mit Personalmangel, sondern auch die Wirtschaft.

Nur gemeinsam stark

Um der Datenflut Herr zu werden, setzt die Polizei auf die enge Zusammenarbeit mit internationalen Software-Unternehmen, Dienstleistern oder Universitäten. »Nur wenn wir das Problem gemeinsam angehen, können wir etwas bewegen. Durch Kooperationen und Hospitationen tauschen wir unser Wissen aus und arbeiten gemeinsam an Lösungen, besonders im Bereich Speicherkapazität und Analysetools«, erklärt Helmut Picko vom Cybercrime-Kompetenzzentrum. So werden etwa ständig die neuesten Technologien für die Auswertung von großen Datenmengen auf ihre Einsatzfähigkeit bei der Polizei geprüft. Aber auch Unternehmen aus anderen Wirtschaftszweigen können bei der Bewältigung von großen Datenmengen hilfreich sein. »Wir tauschen uns zum Beispiel mit den IT- und Geschäftsverantwortlichen der Unternehmen regelmäßig aus, da auch dort große Datenmengen anfallen, die bewältigt werden müssen – hier können wir voneinander lernen«, so Picko. Auch der Austausch mit internationalen Polizeien sei wichtig. Hier seien jedoch häufig die unterschiedlichen Rechtsgrundlagen ein Problem. »Nur weil etwas im Ausland technisch gut funktioniert, heißt das nicht, dass wir diese Maßnahmen einfach so übernehmen können, da bei uns zum Beispiel mit dem Thema Datenschutz rechtlich ganz anders umgegangen wird«, betont Andreas Lezgus.

Semantische Analyse hilft bei Ermittlungen

Auch die »semantische Analyse« kann für den polizeilichen Einsatz hilfreich sein. Im Rahmen einer Hospitation mit einem großen Kommunikations- und Technologieunternehmen hat das LKA NRW bereits den Einsatz dieser Technik erprobt. Dazu wurden Daten – Webseiten, Fotos, E-Mails, Telefonate und Chatverläufe – aus einem bereits abgeschlossenen Ermittlungsverfahren mithilfe einer Software neu ausgewertet, die die Möglichkeiten der semantischen Analyse nutzt. »Diese Software verfügt über eine Sprachintelligenz und ist damit in der Lage, bestimmte Informationen und Fragestellungen, die wir ihr vorgeben, auf die zugrundeliegenden Daten anzuwenden«, erklärt Dezernatsleiter Helmut Picko. »Sie prüft im Anschluss, welche Daten eine hohe Übereinstimmung mit unseren Fragestellungen haben und filtert diese Daten heraus. Die Software kann also so programmiert werden, dass sie das Kriminalitätsphänomen, um das es geht, versteht, und nach den Dateien sucht, die damit im Zusammenhang stehen könnten«, so der Experte. Heraus kommt dabei eine Datenmenge, die anschließend von einem Sachbearbeiter auf ihre tatsächliche Relevanz für den Fall gesichtet werden kann. Helmut Picko: »Auf den menschlichen Sachverstand eines polizeilichen Ermittlers wird man auch in Zukunft nicht verzichten können. Aber man kann – und muss – die Kolleginnen und Kollegen mithilfe solcher Programme unterstützen. Ansonsten sind die großen Datenmengen in Zukunft nicht mehr zu bewältigen.«

IT-Strategie ist kein Zufall

Die zunehmende Digitalisierung kompletter Prozesse hat große Auswirkungen auf alle polizeilichen Aufgabenbereiche und wird diese verändern. Neue digitale Produkte im Halbjahreszyklus, der wachsende Einfluss der Konsumententechnologien, tragbare Sensoren, 3D-Drucktechnologien und neue Analysetechniken für die damit verbundenen enormen Datenmengen sind nur einige Beispiele für die Innovationstreiber. Es muss intensiv geprüft werden, welche etablierten Verwaltungsprozesse auf die wachsende Geschwindigkeit von technologischen Veränderungen angepasst werden müssen. Daher ist es besonders wichtig, dass zukünftig alle Führungskräfte die Potenziale und Auswirkungen der neuen Technologien verstehen und hierzu die notwendigen Organisationsveränderungen umsetzen. Um eine große Organisation wie die Polizei NRW hierbei IT-strategisch richtig in die Zukunft führen zu können, bedarf es der genauen Auswertung von Marktanalysen und Forschungsergebnissen. Denn man muss wissen: Wo geht der technologische Trend hin? Welche Entwicklungen sind für die Polizei in welchen Zeiträumen relevant? Wie ist die veränderte Erwartungshaltung der Gesellschaft? Der Aufwand, der dazu nötig ist, wird häufig unterschätzt. »Ein neues Projekt mit Änderungen in den Strukturen einer solch großen Organisation dauert immer zwischen zwei und fünf Jahren. Wenn wir dabei strategisch in eine falsche Richtung gehen, können wir das nur noch mit einem erheblichen zusätzlichen finanziellen und personellen Aufwand aufholen. Deshalb ist es erfolgskritisch, dass wir uns frühzeitig gemeinsam mit den Fach- und IT-Verantwortlichen mit den Schwerpunkten im IT-Bereich der Polizei befassen, um uns entsprechend für die Zukunft aufzustellen«, betont Andreas Lezgus. ///

Simone Wroblewski

BIG DATA IST HEUTE – NEUER DATENSPEICHER IM LKA NRW

»Mehr als 640 Kilobyte werden Sie niemals benötigen!« (Bill Gates, 1981) – diese Aussage des Computerpioniers gilt inzwischen als eine der bekanntesten Fehleinschätzungen in der Geschichte der technischen Entwicklung. Jedes Handyfoto hat mittlerweile schon eine Größe von mehr als einem Megabyte.

Das Cybercrime-Kompetenzzentrum im LKA NRW arbeitet seit 2015 mit einem Datenspeicher einer ganz anderen Dimension. Das sogenannte »Hybrid RAID System« ist ein Verbund von mehreren Hundert Festplatten. Derzeit stehen darauf netto 300 Terabyte als ein Laufwerk zur Verfügung, auf dem Daten Plattform übergreifend zeitgleich gespeichert und analysiert werden können. Bei Bedarf kann das System auf 4.000 Terabyte (4 Petabyte) aufgestockt werden. Zum Vergleich: Ein handelsüblicher Computer kann auf seiner Festplatte etwa zwei Terabyte speichern.

»Eine herausragende Eigenschaft des Systems ist die hohe Geschwindigkeit. Zehn Terabyte können in circa 50 Minuten kopiert werden. Wichtige Daten stehen den Ermittlern dadurch schneller zur Verfügung«, so Dezernatsleiter Helmut Picko über den neuen Superspeicher. Wobei die Datenmenge nach der Sicherung immer noch unübersichtlich groß sein kann. Ein Terabyte würde als Druckwerk etwa 550.000 Büchern zu 500 Seiten entsprechen. »Das verdeutlicht, dass unsere Ermittler diese Beweise nicht wie eine Tatwaffe untersuchen oder wie eine Papierakte durchlesen können«, so Helmut Picko weiter. »Ein großer Datenspeicher braucht Programme, die diese Menge für den Menschen überschaubar machen und das Wichtige vom Unwichtigen trennen.«

Inzwischen experimentiert das Kompetenzzentrum mit hochentwickelter Software, die durch Eingaben der Ermittler eine phänomentypische Sprache lernen können. »Je nachdem, in welchem Kontext ein Wort auftaucht, erkennt das Programm, ob es sich um Begriffe aus dem Bereich des Kindesmissbrauchs oder um harmlose Teenagerkommunikation handelt, ob man über Cannabis plaudert oder einen tatsächlichen Drogenhandel plant«. Am Ende der Analyse durch die Software sollte der Ermittler nur noch die Informationen lesen, die für das Verfahren von Bedeutung sein können. Ein Test mit umfangreichen Daten aus einem abgeschlossenen Ermittlungsverfahren hat gezeigt, dass auf diese Weise aus über 50.000 Seiten Text die vier Seiten herausgefiltert werden konnten, die auf die Spur der Täter führten.

Das neue große Storage-System wird seit 2015 im LKA NRW betrieben, denn 640 Kilobyte reichen schon lange nicht mehr aus! /// ***Christian Mirgel, LKA NRW***

Handarbeit statt Softwareprogrammierung

Kooperation mit der Fachhochschule Aachen beschert Cybercrime-Kompetenzzentrum neuen Mitarbeiter

Philip Schütz wollte zu Beginn seines Informatikstudiums eigentlich Softwareprogrammierer werden. Doch als er im Rahmen einer Kooperation des Landeskriminalamtes NRW mit der Fachhochschule Aachen ein Praxissemester im Cybercrime-Kompetenzzentrum absolvierte, änderte er seinen Berufswunsch. Heute arbeitet er in der Landeszentrale IuK-Ermittlungsunterstützung beim Landeskriminalamt NRW.

Auf dem linken Schreibtisch steht ein normaler Computer, davor liegen Umlaufmappen und Zettel. Auf dem rechten Schreibtisch stehen auf einem Aufbau lauter offene kleine blaue Kisten, in denen in ihre Einzelteile zerlegte Handys liegen. Darunter kleines Werkzeug, ein unscheinbarer schwarzer Kasten und ein Koffer voller Adapter. Bunte Gitarrenplättchen in unterschiedlicher Stärke liegen auf dem Tisch. An den Wänden hängen Architektur- und Landschaftsaufnahmen. Dies ist das Reich des 27-jährigen Informatikers Philip Schütz. Seit März 2013 verstärkt er das Sachgebiet 43.1 des Landeskriminalamtes NRW (LKA NRW). Zu ihm kommen die schweren Fälle, die auf den ersten Blick hoffnungslos wirken: Handys mit kaputtem Display, vom Feuer geschmolzene Hüllen, zerstörte USB-Zugänge. Wenn die Experten in den Kreispolizeibehörden bei elektronischen Geräten nicht mehr weiter kommen, senden sie diese an die Landeszentrale IuK-Ermittlungsunterstützung. Das können Computer sein, Handys, Navigationsgeräte

Fotos (2): Jochen Tack

Rework Station zum Auslöten von Speicherchips

oder auch POS-Terminals, mit denen man in Geschäften mit EC-Karten oder Kreditkarten zahlen kann. Die Spezialisten können dann so manchen Datenträger noch auslesen, der zuvor hoffnungslos aussah. Manchmal reicht dazu schon das spezielle Auslesegerät, als das sich der unscheinbare schwarze Kasten entpuppt, der auf dem Schreibtisch steht, um recht schnell an die Daten zu gelangen. »Bei anderen Fällen dauert es Tage und erfordert einiges an Handarbeit und Kreativität, bis wir die benötigten Inhalte zur Verfügung stellen können«, erklärt Philip Schütz. Dabei kommen unter anderem auch die Gitarrenplättchen zu Einsatz, denn mit ihrer Hilfe lassen sich Handyhüllen leichter öffnen. Und manchmal müssen auch sie passen.

Vom Hörsaal ins Cybercrime-Kompetenzzentrum

Begonnen hatte für den Informatiker alles mit einer Vorlesung zu IT-Forensik während seines Bachelorstudiums an der Fachhochschule Aachen (FH Aachen). Das Thema fesselte ihn und als er erfuhr, dass man ein Praxissemester dazu machen kann, entschied er sich dafür. Er hatte die Wahl zwischen einem Unternehmen und dem LKA NRW. »Die Entscheidung fiel mir nicht schwer«, berichtet er, »ich fand die Polizei viel spannender.« Und so kam er Anfang 2012 gemeinsam mit einem Kommilitonen als erster Student des Fachbereichs Elektrotechnik und Informationstechnik der FH Aachen zum Cybercrime-Kompetenzzentrum. Vier verschiedene Themen schlug das LKA NRW den beiden Studenten vor. Da sie gerne gemeinsam an einem Thema arbeiten wollten, entschieden sie sich

Philip Schütz, Informatiker im Cybercrime-Kompetenzzentrum

dafür, eine Mobilfunkzelle im kleinen Maßstab aufzubauen, um anschließend Experimente damit durchführen zu können. Funkzellen empfangen und senden Daten und ermöglichen so die Kommunikation mit einem Handy. Die Mobilfunkzelle sollte so offen sein, dass man Daten unproblematisch auslesen kann und sie sollte auch nicht zu kostspielig sein.

Handytrojaner-Analyse mithilfe einer Mobilfunkzelle

Die beiden Studenten konnten die Anforderungen erfüllen und bauten eine kleine Mobilfunkzelle, die auch heute noch im LKA NRW im Einsatz ist. Dann verfolgte jeder sein eigenes Projekt weiter. Während sich sein Kommilitone damit beschäftigte, wie man ein Handy mit Hilfe der Mobilfunkzelle mit Daten befüllen kann, wandte sich Philip Schütz der Analyse von Handytrojanern zu. »Wenn man den Trojaner hat, kann man ihn analysieren«, erklärt der LKA-Mitarbeiter. »Es kann aber auch sein, dass man nur ein Handy hat, bei dem ein Trojaner vermutet wird. Dann muss man das Verhalten analysieren, um herauszufinden, ob das Handy tatsächlich infiziert ist und wie der Trojaner funktioniert.« Dazu meldet er das betroffene Handy bei der Mobilfunkzelle an und versucht etwa durch das Aufrufen von Apps verdächtiges Verhalten zu provozieren. Dabei analysiert er zum Beispiel, ob das Handy SMS an bestimmte Nummern schickt oder Daten an bestimmte Server. Um das Auslesen der Daten zu erleichtern, hat der Informatiker ein Programm geschrieben, das die Auswertung erleichtert. Auch dieses Programm ist heute noch im Einsatz. Über dieses Projekt hat er auch seine Bachelorarbeit geschrieben, für die er eine glatte eins bekommen hat.

Stellen für Informatiker bei der Polizei sind noch selten

Als beim LKA NRW kurz darauf eine Stelle als IT-Sachbearbeiter ausgeschrieben war, hat er nicht lange gezögert und sich beworben. »Eigentlich hatte ich geplant, noch einen Master zu machen«, berichtet er. »Doch ich wusste, dass solche Stellen rar sind und daher habe ich die Gelegenheit ergriffen und mich beworben.« Er musste eine normale Bewerbung durchlaufen, inklusive Assessment-Center. Seit etwas mehr als zwei Jahren bearbeitet er nun die kniffligen Vorgänge aus dem ganzen Land und hat seine Entscheidung noch keine Minute bereut. Wer dem freundlichen 27-Jährigen auf der Straße begegnet, würde wohl nicht als erstes denken, dass er einem Informatiker gegenüber steht. Mit seinem offenen Wesen, den trendigen Turnschuhen und dem karierten Hemd würde man wohl eher auf die Kommunikationsbranche oder gar Betriebswirtschaft tippen. Seine guten kommunikativen Fähigkeiten kommen ihm in seiner neuen Stelle zugute. Schließlich muss er häufiger mal Kollegen ohne technischen Hintergrund erklären, warum etwas geht oder eben auch nicht. Im Januar 2014 hat er seine Ausbildung zum Gutachter begonnen, damit er seine Analysen bald auch vor Gericht vertreten kann.

Zahlenkolonnen und Handarbeit

»Mein Alltag ist sehr abwechslungsreich«, erklärt er. »Ich lese Daten aus Handys aus und analysiere sie. Dabei muss ich manchmal auch ganz neue Wege beschreiten, um zum Ziel zu kommen. Wer hier arbeitet sollte schon gerne basteln und tüfteln«, sagt er mit einem Schmunzeln. Als großen Handwerker bezeichnet er sich nicht. »Mir liegt da eher die Arbeit mit dem Mikroskop im Kleinen als das Hantieren mit großen Geräten«, sagt er. Das Handwerkliche hat er vor allem gelernt, indem er älteren Kollegen über die Schulter geschaut hat. »Etwas derartiges vermittelt das Studium nicht«, berichtet er. Er schätzt die kollegiale Zusammenarbeit und die unterschiedlichen Hintergründe seiner Kollegen. »Wir sind hier zur Hälfte Informatiker und Techniker und zur Hälfte Polizeivollzugsbeamte. Das ergänzt sich sehr gut.« Der Sachgebietsleiter Dietmar Scheffler ist froh über die jungen Mitarbeiter: »Ältere Beschäftigte können natürlich auf einen ganz anderen Fundus an Erfahrungen blicken, doch die jungen Mitarbeiter bringen eine ganz andere Sichtweise ins Sachgebiet, die uns gut tut.« /// ***Katerina Breuer***

KOOPERATION ZWISCHEN DER FH AACHEN UND DEM LKA NRW

Seit Ende 2011 besteht eine Kooperation zwischen dem Fachbereich Elektrotechnik und Informationstechnik der FH Aachen und dem Cybercrime-Kompetenzzentrum des LKA NRW. Informatikstudenten können seitdem ihr Praxissemester im LKA NRW absolvieren und dabei ein Thema bearbeiten, das die Landeszentrale IuK-Ermittlungsunterstützung zuvor als sinnvoll für die Polizeiarbeit identifiziert hat. »Wir wurden von Studierenden recht stark in Anspruch genommen – ohne davon zu profitieren«, erläutert Dietmar Scheffler, Sachgebietsleiter des SG 43.1 Landeszentrale IuK-Ermittlungsunterstützung. »Im Rahmen dieser Kooperation können wir die Themen auswählen, die die Studenten bearbeiten. So profitieren jetzt beide Seiten.« Doch das ist nicht der einzige Vorteil der Zusammenarbeit: Bei besonders schweren Einzelfällen können sich die LKA-Mitarbeiter direkt an die Experten der FH Aachen wenden. Und manchmal finden sie gemeinsam tatsächlich eine Lösung. Durch die Praxissemester und die darauf aufbauenden Abschlussarbeiten der Studenten wurden schon neue Technologien entwickelt, die heute tatsächlich im Einsatz sind. Und schließlich unterstützt die Kooperation den Wissenstransfer im Bereich der Sicherheit und Forensik von IT-Systemen. Die FH Aachen hat dadurch einen spannenden Partner für ihre Studenten gewonnen und kann sich bei Fragen direkt an das LKA NRW wenden. »Wir bekommen sehr gute Rückmeldungen von den Studenten. Offenbar fühlen sie sich bei uns gut aufgehoben«, sagt der Sachgebietsleiter. Zurzeit ist wieder ein Student im LKA NRW. Er beschäftigt sich mit der Untersuchung von Mobiltelefonen. Mit ihm haben dann schon sieben Studierende dieses Angebot in Anspruch genommen.

PRÄVENTIONS-TIPP

SCHUTZ VOR VIREN UND TROJANERN, BOT-NETZEN UND RANSOMWARE

> Achten Sie auf einen umfassenden Grundschutz Ihres Computers: ein aktueller Virenscanner, eine aktivierte Firewall, ein aktuell gehaltenes Betriebssystem und ein Webbrowser in der jeweils neuesten Version.
> Öffnen Sie niemals ungeprüfte Dateianhänge von E-Mails.
> Vermeiden Sie, auf Links in zugesandten E-Mails zu klicken. Dies gilt in besonderem Maß für E-Mails, die unaufgefordert geschickt wurden.
> Löschen Sie verdächtige Mails ungelesen.
> Seien Sie misstrauisch bei Mitteilungen oder Angeboten in Sozialen Netzwerken von Ihnen nicht bekannten Teilnehmern.
> Erstellen Sie regelmäßig Backups Ihrer wichtigsten Dateien auf externen Datenträgern oder – besser noch – ein komplettes Systemabbild.

Videos zu diesen Tipps finden Sie im Internet unter: www.sichere-netzwelten.de

PERSONALWERBUNG

Arbeiten im Cybercrime-Kompetenzzentrum

Eine hohe IT-Affinität ist Voraussetzung

Markus Röhrl, Leiter der Abteilung 4 beim Landeskriminalamt Nordrhein-Westfalen, über die Herausforderung, neue Mitarbeiterinnen und Mitarbeiter zu finden, und die erfolgreiche Zusammenarbeit von Kriminalisten und IT-Spezialisten.

Streife: Welche Voraussetzungen sollte man mitbringen, wenn man beim Cybercrime-Kompetenzzentrum arbeiten möchte?
Röhrl: Man muss nicht schon ein fertiger Cyberkriminalist sein, um bei uns anzufangen. Es muss auch nicht jeder Mitarbeiter IT-Forensiker werden, wir haben hier sehr vielseitige Aufgaben. Man sollte aber eine hohe IT-Affinität und Lust auf die Bekämpfung von Cybercrime mitbringen.

Streife: Wie haben Sie qualifizierte neue Kolleginnen und Kollegen gefunden?
Röhrl: Von den rund 100 Beschäftigten im Cybercrime-Kompetenzzentrum sind etwa 30 Stellen neu geschaffen worden. Es ist schwierig, erfahrene Spezialisten zu bekommen. Einige wenige sind aus den Behörden gekommen. Zusammen bilden die Erfahrenen das Rückgrat des Cybercrime-Kompetenzzentrums. Ansonsten haben wir nach jungen Polizeibeamten mit besonderem Potenzial oder nachgewiesenen Fähigkeiten wie etwa einer Berufsausbildung oder einem Studium im IT- oder Medienbereich gesucht. Im Wach- und Wechseldienst, aber auch bei den Einsatzhundertschaften sind wir fündig geworden. Und wir haben Regierungsbeschäftigte mit einem abgeschlossenen Informatikstudium eingestellt, um unsere Expertise noch zu erweitern.

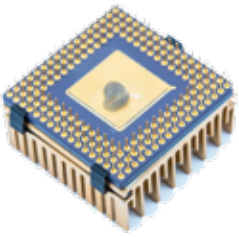
Streife: Wie integrieren Sie diese hohe Anzahl an jungen neuen Beschäftigten?
Röhrl: Viele junge Kollegen bedeuten gerade in den Anfangsjahren für die erfahrenen Mitarbeiterinnen und Mitarbeiter auch eine persönliche Belastung. Diese Herausforderung haben die Spezialisten aber neben ihrer Verantwortung für die Kernprozesse gerne angenommen. Polizeibeamte ohne Erfahrung in der Kriminalitätssachbearbeitung schicken wir zunächst in die sechsmonatige Einführungsfortbildung. Danach folgen spezialisierte Module beim LAFP NRW und ein intensives Learning-on-the-Job in den Ermittlungskommissionen. Ich bin mir sicher, in drei bis vier Jahren werden die jungen Mitarbeiterinnen und Mitarbeiter bereits sehr gute Cyberkriminalisten sein. Aber weitere Qualifizierungen werden folgen müssen, international wie national.

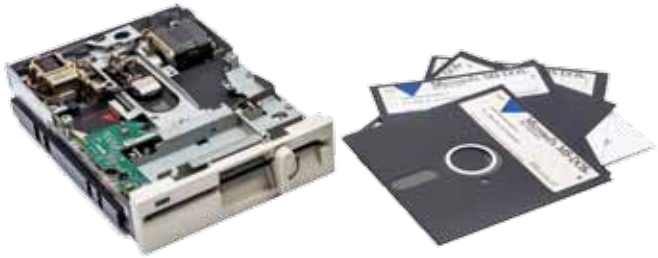

Foto: Landeskriminalamt NRW

Streife: Sie hatten es bereits angesprochen: Im Cybercrime-Kompetenzzentrum arbeiten auch studierte Informatiker. Warum braucht die Polizei in diesem Bereich extern erworbenes Wissen?
Röhrl: In den Aufgabenbereichen des Cybercrime-Kompetenzzentrums gibt es rasante technische Entwicklungssprünge. Wir brauchen Mitarbeiterinnen und Mitarbeiter, die wissenschaftlich vertiefte Grundkenntnisse haben und besondere technische Problemlösungen am Fall entwickeln können. Erst die Verzahnung von hoher technischer Intelligenz mit spezifischen fachkriminalistischen Fähigkeiten begründet die besonderen Erfolge in herausragenden Verfahren. ///

Das Interview führte Katerina Breuer

Fotos: Jochen Tack





Als noch mit Diskette und Kassettenrekorder gearbeitet wurde

Cybercrime gestern und heute

Der 2014 pensionierte Leiter der Dienststelle Computerkriminalität Ulrich Bahlo erinnert sich noch an die ersten Computer, die bei der Polizei in Münster eintrafen, und an die Zeit, als Massendaten auf Disketten gespeichert wurden.

Die News war den »Westfälischen Nachrichten« im Jahr 1994 einen halbseitigen Artikel wert: Die Polizei Münster wird ganze 13 Jahre nachdem IBM den ersten Personal Computer (PC) vorgestellt hatte, mit 28 PCs und neun Laserdruckern ausgestattet. An eine Vernetzung der Computer untereinander oder gar mit anderen Behörden war 1994 noch nicht zu denken. Der damalige zuständige Sachgebietsleiter Ulrich Bahlo war trotzdem begeistert und berichtete in der Zeitung: »Der übliche Schreibkram geht viel schneller von der Hand, den Kollegen bleibt mehr Zeit für die Arbeit im Außendienst.« In Vier-Tages-Schulungen wurden die Beschäftigten damals mit der Arbeit an einem PC vertraut gemacht. Bei vielen hat diese »moderne« Technik nicht gerade Begeisterung geweckt. Es war das gleiche Jahr, in dem in den USA zwei Anwälte den Startschuss setzen für den profimäßigen Versand von Spam-Mails.

Wenn Ulrich Bahlo an diese Zeit zurückdenkt, muss er schmunzeln. 1990 hatte die Polizei Münster ihre allerersten fünf Rechner erhalten – damals noch terminalbasiert. Die heutige Durchdringung des Internets in alle Lebensbereiche hätte sich in Deutschland keiner vorstellen können. Gerade einmal zehn Jahre zuvor hatte die Universität Karlsruhe die erste deutsche Mail überhaupt empfangen. Den gelernten Fernmeldetechniker interessierte diese neue Technik von Anfang an. Nach seinem Einstieg bei der Bereitschaftspolizei und mehreren Jahren im Wach- und Wechseldienst, war er seit 1982 für die technische Ausstattung der Polizei Münster zuständig, seit 1986 als Sachgebietsleiter.

Erste IT-Anwendung brach im Ernstfall zusammen

Er erinnert sich noch sehr gut daran, wie in Münster die erste IT-Anwendung zum Einsatz kam. Es war 1997, die Zeit der Castor-Transporte. Durch die Vernetzung von mehreren PCs hatten sie ein internes Netzwerk aufgebaut, auf dem ein digitales Kräfteberechnungsprogramm laufen sollte. »Während des Einsatzes brach das Programm dann zusammen und wir mussten doch wieder analog arbeiten«, erinnert sich der 62-Jährige. Er denkt gerne an diese Anfangszeit zurück, in der Pionierarbeit geleistet wurde, wie er es nennt. »Damals musste man sich vieles, was heute selbstverständlich ist, hart erarbeiten. Vieles geschah zum ersten Mal.«

Sein erster Fall, bei dem Telefon, Mail und Erpressung verknüpft waren, geschah um das Jahr 2000. Damals erpresste ein Täter einen Discounter mit Hilfe einer virtuellen Rufnummer und eines Mail-Accounts, der mit erfundenen Daten bestückt war. Somit liefen die normalen Ermittlungen zunächst ins Leere. Die einzige greifbare Spur war ein Indianername, den er nutzte. Tagelang überwachten sie rund um die Uhr die Datenströme, um dem Täter live aufzulauern. Als der Indianername schließlich endlich wieder auftauchte, konnten sie ihn bis in ein Kaufhaus in Münster zurückverfolgen, wo damals noch frei zugängliche Internetrechner standen. Die Einsatzkräfte, die sofort dorthin gerufen wurden, konnten den Erpresser auch tatsächlich festnehmen. »Das war schon ein gutes Gefühl, als wir ihn dann endlich hatten«, sagt Ulrich Bahlo. >

Fotos (2): Jochen Tack

Ulrich Bahlo, ehemaliger Leiter der Dienststelle Computerkriminalität in Münster

Infiziert mit dem IuK-Virus

Zwei große Arbeitsgruppen gab es in Nordrhein-Westfalen, die sich schon frühzeitig mit Computerkriminalität befassten und versuchten, die Polizei auf diese neue Herausforderung vorzubereiten. »Die Mitglieder dieser ersten Arbeitsgemeinschaft, die ab dem Jahr 2000 arbeitete, waren alle vom IuK-Virus infiziert, wie ich das nenne«, sagt der Pensionär. »Zahlreiche Kollegen, die mit mir dort gearbeitet haben, sind auch heute noch in diesem Bereich tätig, wie Helmut Picko, der mittlerweile Dezernatsleiter im Cybercrime-Kompetenzzentrum des Landeskriminalamtes ist.« Während in der Frühzeit die Auswertung und Analyse der IuK-Kriminalität, wie es kurz für Information und Kommunikation heißt, meist bei den Technikdienststellen war, merkte man schnell, dass ein Bezug zur Kriminalpolizei nicht fehlen darf. Die Polizei Münster reagierte 1999 und siedelte die Auswertung von IuK-Spuren bei der Kriminalpolizei an. Ulrich Bahlo übernahm die Leitung. Im Jahr 2002 wurden die IT-Forensik und im Jahr 2004 die IuK-Kriminalitätssachbearbeitung ebenfalls in diesem Arbeitsbereich integriert.

Sein Team setzte sich zunächst aus vier weiteren Mitarbeitern zusammen, die alle mit vollem Herzblut bei dem Thema waren. Viele dieser Kollegen hatten sich ihr Wissen gerade in der Anfangszeit privat angeeignet. Das Kernteam ist ihm sein restliches Arbeitsleben treu geblieben. »Die Kollegen haben sich so in das Thema eingearbeitet, dass sie zu absoluten Spezialisten geworden sind. Dafür hat der eine oder andere auch auf eine Karriere verzichtet«, berichtet er. In seinem Arbeitsbereich galt das Wort »analog« als Schimpfwort. »Wenn jemand gesagt hat: `Du denkst aber analog´ war das nicht gerade nett gemeint«, berichtet er lachend. Die Dienststelle wechselte immer wieder ihre Zuordnung innerhalb der Kriminalpolizei, bis 2006 schließlich das KK 22 daraus wurde – mit den Arbeitsbereichen Computerkriminalität, Betrug mittels neuer Medien, IuK-Ermittlungs- und Einsatzunterstützung, Telekommunikationsüberwachung (TKÜ) und IT-Forensik.

Mit PC und Kassettenrekorder wurden Tausende betrogen

Um das Jahr 2000 spielten ganz andere Delikte als heute eine große Rolle. So standen etwa die Ausnutzung von kostenpflichtigen Dialernummern wie 0190 oder auch Urheberrechtsverletzungen in Form von illegalen Downloads im Vordergrund. »In einem Jahr hatten wir damals über 3.000 Ermittlungsverfahren zu illegalen Downloads«, berichtet der zweifache Vater. »Die Staatsanwaltschaft hat uns die Unterlagen damals kartonweise geschickt.« Bei einem der ersten großen Dialer-Verfahren in Münster spielte ein herkömmlicher Kassettenrekorder eine große Rolle: Der Täter hatte günstige Autos angeboten und eine 0190er-Nummer angegeben, unter der man sich bei Interesse melden sollte. Sobald die Opfer anriefen, schaltete sich über PC ein Kassettenrekorder ein, auf dem ein Besetztzeichen abgespielt wurde. Die Interessierten dachten, da der Anschluss besetzt sei, würden sie keine Gebühren bezahlen und versuchten es immer wieder von Neuem. In Wahrheit wurden pro Anruf fünf Euro fällig. »Wir bekamen über 5.000 Rufnummern von Geschädigten«, denkt Ulrich Bahlo zurück, »damals noch auf Disketten. Wir haben extra Programme schreiben lassen, damit wir nicht jede Nummer einzeln anpacken mussten, um die Anschlussinhaber zu ermitteln.« Im Vergleich zu heute sind das kleine Mengen. Während seine Dienststelle 2005 ein Datenvolumen von 18 Terabyte gesichert und ausgewertet hat, waren es 2013 schon 250 Terabyte.

Heutige Probleme reichen weit zurück

Beleidigungs- und Bedrohungsdelikte über das Internet kamen um das Jahr 2000 gerade so auf, genauso wie Auktionsbetrügereien. Was für den IuK-Ermittler gleich geblieben ist, ist das Kribbeln bei Einsatzlagen. Wenn man besser sein will als sein Gegenüber – einfach nur, um ihn kennenzulernen. »Irgendwann macht schließlich jeder einen Fehler«, sagt der IT-Experte. Die Delikte und Maschen wechselten mit der Zeit immer schneller. Die Täter wurden immer professioneller. »Das Spannende bei Cybercrime ist, dass man nie aufhört zu lernen«, findet Ulrich Bahlo. »Bei einem IuK-Ermittler kann man quasi jedes halbe Jahr die geistige Festplatte löschen und wieder neu bespielen – so schnell sind die Änderungen im rechtlichen, taktischen und technischen Bereich.«

Dabei reichen die Probleme, die auch heute noch eine große Rolle im Internet spielen, zum Teil bis in die Anfangszeit zurück. So wurde schon in einer Doktorarbeit von 1984 ein funktionierender Virus in der Theorie präsentiert, die Praxis folgte bald. Der erste Computerwurm »Morris« hatte 1988 zwar keine direkte Schadenroutine, legte wegen seiner aggressiven Verbreitungsweise aber rund zehn Prozent des damaligen weltweiten Netzes lahm. »Früher brauchte man noch spezielles Wissen, um tätig zu werden«, sagt Ulrich Bahlo. »Je mehr die Technik in die Fläche geht, desto weniger Spezialwissen brauche ich, um Schaden anzurichten. Wie ein einfacher Virus oder Wurm zu programmieren ist, findet heute jeder im Internet.«

Jeder muss Verantwortung übernehmen

Das Thema lässt ihn auch nach seiner Pensionierung nicht los. Er ist nach wie vor mit voller Leidenschaft dabei, lässt keine Artikel zu dem Thema ungelesen. »Ich habe einfach das Glück gehabt, mein Hobby zum Beruf zu machen«, sagt er. Bis zum letzten Arbeitstag hat er noch voll mitgearbeitet. Er erinnert sich an seine Abschiedsfeier: »Die Kollegen haben gesagt: Ulli, du hast uns alles gesagt und es auch schriftlich fixiert – du kannst dir sicher sein, dass hier in nächster Zeit noch alles in deinem Sinne weiterlaufen wird.«

Und dann wird Ulrich Bahlo noch einmal nachdenklich. Man merkt, wie stark ihn das Thema Cybercrime beschäftigt. »Es kann nicht nur Aufgabe der Polizei sein zu ermitteln, wenn das Kind schon in den Brunnen gefallen ist. Schließlich handelt es sich um ein gesamtgesellschaftliches Phänomen. Ich bin der Meinung, dass jeder auch Verantwortung für seine Sicherheit im Netz übernehmen muss. Und auch Prävention darf nicht nur ein polizeiliches Thema sein, auch die Wirtschaft muss stärker vorbeugend agieren«, appelliert er. ///

Katerina Breuer

Löten, fräsen, selber bauen

Foto: Jochen Tack

Die Arbeit der Forensik-Experten im Cybercrime-Kompetenzzentrum

Handys, Smartphones oder Navigationsgeräte enthalten oft Daten, die für Ermittlungen von großer Bedeutung sein können. Welche Nachrichten sind verschickt worden? Hat ein Tatverdächtiger zu einem bestimmten Zeitpunkt telefoniert? Mit wem stand er in Kontakt? Das sind beispielsweise Fragen, die es zu beantworten gilt. Sind die Geräte in einem gutem Zustand und die SIM- und Speicherkarten unbeschädigt, können die jeweiligen Daten in den Polizeibehörden meist eigenständig ausgelesen werden. Gibt es an den Speichermedien jedoch Beschädigungen oder ist das Modell besonders exotisch oder gut gesichert, wird es komplizierter. Dann kommen sie ins Spiel: Die Forensik-Experten des Cybercrime-Kompetenzzentrums im Landeskriminalamt (LKA) NRW.

Fotos (3): Jochen Tack

Ein falscher Handgriff beim Löten kann dazu führen, dass alle Daten unbrauchbar werden.

Zunächst versuchen die Mitarbeiter des Sachgebietes 43.1 »Landeszentrale IuK-Ermittlungsunterstützung« mit möglichst sanften Methoden an die jeweiligen Daten zu kommen. Interessant kann dabei potenziell alles sein: Gespeicherte Kontaktdaten, SMS-Nachrichten, WhatsApp- oder Facebook-Chats oder auch Fotos. Mit verschiedenen Verbindungskabeln und Adaptern wird versucht, das Handy an ein Datensicherungsgerät anzuschließen. Mit etwas Glück können dann sämtliche Handydaten mit Hilfe einer speziellen Software auf einen Rechner heruntergeladen werden. »Das funktioniert leider nicht bei allen Handys oder Smartphones. Manche Geräte sind zum Beispiel so beschädigt, dass die Daten über normale Verbindungen nicht mehr zu extrahieren sind. Dann kommt eine spezielle Kontaktiereinheit zum Einsatz«, erklärt Philip Schütz, Informatiker und seit zwei Jahren beim Cybercrime-Kompetenzzentrum beschäftigt. In die Kontaktiereinheit wird die Handyplatine eingespannt und federnd gelagerte Nadeln werden auf die kleinen Kontakte des Handyspeichers gesetzt. Die Nadeln werden mit einem Rechner verbunden, mit dem dann im Idealfall die Daten ausgelesen werden können, die auf dem Handy gespeichert sind. Dann beginnt jedoch für die Forensiker erst die richtige Arbeit: Denn die Daten werden nicht als Klartext, sondern als zunächst unverständliche lange Zahlen- und Buchstabenfolge dargestellt, die erst einmal entschlüsselt werden muss. »Das ist wie ein großes Puzzle, das mühsam zusammengesetzt werden muss und kann durchaus einige Tage in Anspruch nehmen«, erklärt der Computerexperte.

Löten im Labor

Wenn man auch mithilfe der Kontaktiereinheit nicht weiterkommt, müssen die Forensiker zu härteren Mitteln greifen. Im Labor haben die Experten die Möglichkeit, die Platinen selbst mit einem Lötkolben zu bearbeiten. Dafür braucht man viel Fingerspitzengefühl und eine ruhige Hand, denn die genutzten Drähte haben zum Teil nur einen Durchmesser von 0,02 mm – also etwa die Hälfte des Durchmessers eines Haars. Mit Pinzette, Lötzinn und Lötkolben wird nun unter dem Mikroskop versucht, die Drähte an den richtigen Punkten auf der Handyplatine zu befestigen, damit über die Drähte wiederum die Daten ausgelesen werden können. »Über die so genannte JTAG-Schnittstelle versuchen wir, an die Daten auf der Platine zu kommen. Diese Schnittstelle ist aber auf jeder Platine anders angelegt. Daher müssen wir vorab recherchieren, wo die Schnittstelle bei dem einzelnen Handy- oder Navigationsgerät zu finden ist«, erklärt Philip Schütz. Dabei hilft oft nur die Internetrecherche oder die direkte Anfrage beim Hersteller. Ein falscher Handgriff beim Löten kann dazu führen, dass alle Daten auf dem Chip unbrauchbar werden. »Beim Lötvorgang entsteht eine so große Hitze, dass der Chip komplett zerstört wird, wenn man die Platine zu lange bearbeitet«, erklärt Schütz. Und selbst wenn man es geschafft hat, die Drähte an den richtigen Stellen auf dem Chip zu platzieren, kann noch etwas schiefgehen. »Die entstandene Verbindung aus Chip und feinen Drähten ist so empfindlich, dass man umgehend versuchen muss, ob man die Daten nun auslesen kann – denn besonders langlebig ist die Konstruktion nicht«, betont der Experte.

Learning by doing

Da jeder Handy- und Smartphonehersteller die Daten auf seinen Geräten anders ablegt und es sogar für die verschiedenen Handymodelle eines einzigen Herstellers unterschiedliche Möglichkeiten dazu gibt, besteht häufig nicht die Möglichkeit einer einheitlichen Vorgehensweise beim Auslesen von Handy-Daten. »Wir müssen oft erst herausfinden, wie die Daten überhaupt auf dem Handy abgelegt werden und wo etwa Nachrichten gespeichert werden. Dazu nutzen wir Vergleichshandys«, erklärt Philip Schütz. In einem großen Schubladenschrank finden sich daher hunderte Handys und Smartphones verschiedenster Anbieter – auch Modelle, die bereits zehn Jahre oder älter sind. »Wenn wir ein bestimmtes Handy als Beweismittel vorliegen haben, können wir mit dem jeweiligen Vergleichsmodell erst einmal herumprobieren und feststellen, wie und wo die Daten am besten abzugreifen sind«, erklärt der Informatiker. Passend zu den Handys hängen daher auch hunderte Adapterkabel neben dem Schrank. »Manche Täter nutzen gerne ältere Handymodelle, manchmal sogar

mehrere parallel, weil sie billiger sind als neue Smartphones. Oder man findet noch ein altes Handy in irgendeiner Schublade. Daher macht es Sinn, dass wir auch die alten Modelle in unserem Repertoire haben«, so Schütz.

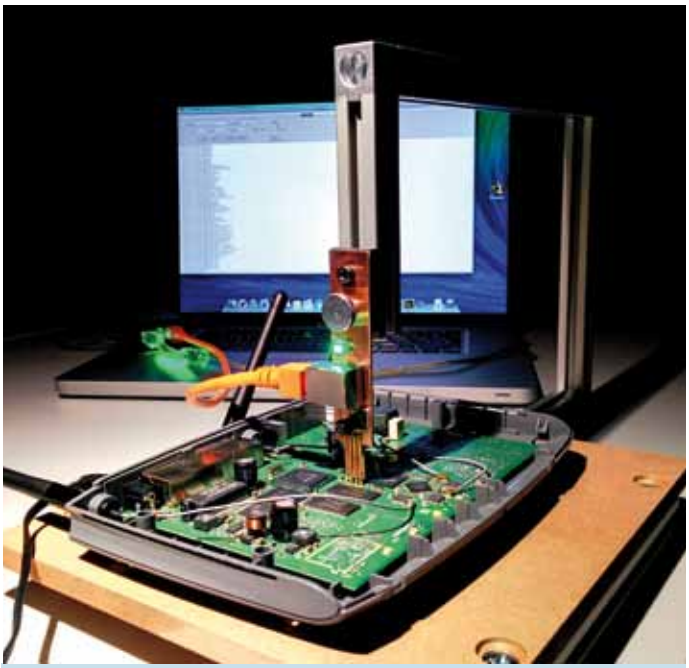
Kein Außenkontakt in der Abschirmkammer

Aber auch Handyviren beschäftigen die Experten. Um diese näher untersuchen zu können, gibt es die »Abschirmkammer«. Dieser kleine Raum ist elektromagnetisch abgeschirmt, das heißt, es ist dort kein Netzempfang möglich. »Die Abschirmung dient dazu, dass bei einer Trojaner-Analyse kein Zugriff von außen auf das zu untersuchende Handy erfolgt«, betont Schütz. Innerhalb der Abschirmkammer kann ein eigenes, unabhängiges Telefonnetz aufgebaut werden. So können die Experten analysieren, wie sich die Schadsoftware verhält oder mit welchem Server sie versucht, Kontakt aufzunehmen. Aber auch wenn man beim Auslesen von Handydaten nicht weiterkommt, kann die Abschirmkammer hilfreich sein. »Wenn ich etwa nicht weiß, in welchem Zahlen- und Buchstabencode SMS auf einem Handychip gespeichert werden, dann kann ich eine eigene Telefonnummer vergeben und selbst eine SMS an ein Vergleichsgerät senden. Zusammen mit der Uhrzeit und dieser Nummer hat man dann zumindest Anhaltspunkte, nach denen man auf dem Chip suchen kann. Hat man die eigenen Daten gefunden, fällt es leichter, auch die anderen Daten zu entschlüsseln, die ja in gleicher Weise abgelegt wurden«, so der IT-Fachmann.

In der »Abschirmkammer« können zum Beispiel Handytrojaner untersucht werden.

Einzelstücke selbst bauen

Mittlerweile steht den Fachleuten auch eine Hochpräzisionsfräse zur Verfügung. Sie arbeitet bis auf einen Mikrometer genau und wird für die Fertigung von speziellen Adapterplatinen genutzt. Forensik-Experte Norbert Paeschel erklärt: »Sobald zum Beispiel von einer Speicherkarte ein oder zwei der Kontaktpads abgebrochen sind, sind die Daten der Karte mit einem gängigen Adapter nicht mehr lesbar. Mithilfe der Fräse kann dann ein Adapter passgenau nachgebaut werden, an den der Speicherchip mit Fädeldraht angelötet und mit normalen Kartenlesern kontaktiert und ausgelesen werden kann. Im normalen Handel sind solche Adapterplatinen nicht zu bekommen.« >



FORENSISCHE AUSWERTEMETHODEN AN DSL-ROUTERN

Eine weitere Unterstützungsleistung des Sachgebietes 43.1 ist das forensische Auslesen von passwortgeschützten DSL-Routern. Hier wurde mangels kommerziell verfügbarer Produkte eine eigene Hardware entwickelt, die es ermöglicht, DSL-Router im laufenden Betrieb auszulesen. Aus dem Prototypen entstand durch gezielte Weiterentwicklung das sicher bedienbare Gerät »Skorpion«, welches nach einer Kleinserienfertigung im Rahmen eines Workshops am 3. März 2015 an die Kriminalhauptstellen ausgegeben werden konnte. Damit sind diese Polizeibehörden jetzt in der Lage, vor Ort ad-hoc Sicherungsmaßnahmen durchzuführen.

Hochpräzisionsfräse beim Fräsen einer Platine

Ein weiterer Anwendungsbereich ist die Herstellung von Kontaktiereinheiten für Speicherchips. Die Fräse bohrt nach einem vorgegebenen Bauplan, dem so genannten Layout, das zunächst an einem Rechner programmiert werden muss, die passenden Bohrungen dazu. Diese dürfen kein Spiel haben, denn im Anschluss werden Kontaktiernadeln von zum Teil nur 0,3 mm Durchmesser in die Bohrungen eingesetzt. Bei dieser Arbeit kommt es auf Geduld, handwerkliches Geschick, aber auch Kreativität an. »Die Produkte, die mit der Fräse gefertigt werden, bieten uns Möglichkeiten beim Auslesen von Daten, die wir vorher nicht hatten. Allerdings müssen wir bei dieser Präzisionsarbeit sehr überlegt und bewusst vorgehen. Deshalb arbeiten wir grundsätzlich nach dem Vier-, besser sogar nach dem Sechs-Augen-Prinzip«, erklärt der Kriminaloberkommissar. Bei seiner Arbeit kommt Norbert Paeschel auch die Zeit vor seinem Wechsel zur Polizei zugute, denn er ist gelernter Werkzeugmacher. »In unserer Abteilung werden viele Wissensbereiche vereint – Informatik, Werkzeug-, Elektro- und Hochfrequenztechnik, Maschinenbau, Layouterstellung – und natürlich die klassische Polizeiarbeit«, betont der Fachmann. Die Forensik-Experten werden auch in den kommenden Jahren viel zu tun haben. Ein nächster Schritt wäre etwa, Platinen mit Lasern zu bearbeiten, wagt Norbert Paeschel einen Blick in die Zukunft. ///

Simone Wroblewski

MANIPULIERTEN SPIELAUTOMATEN AUF DER SPUR

Ebenfalls in den Bereich der Forensik-Experten im Cybercrime-Kompetenzzentrum fallen manipulierte Geldspielautomaten. Diplom-Ingenieur Michael Thelen ist der einzige Gutachter auf Behördenseite in ganz Deutschland, der sich mit diesem Thema befasst. Bei ihm landen daher Fälle aus ganz Deutschland, soweit die Auftragslage aus NRW dies zulässt. »Man braucht für diesen Bereich technisches Verständnis, Erfahrung, aber auch eine gute Kenntnis der Gesetze rund um das Thema Glücksspiel«, erklärt Thelen. Beim Betrug mit Glücksspielautomaten gibt es zwei wichtige Aspekte: Entweder werden Automaten von den Aufstellern so manipuliert, dass die integrierte Software höhere ausgeschüttete Gewinne anzeigt. Denn je mehr Gewinne eine Maschine an Spieler ausgegeben hat, desto weniger Steuern muss der Betreiber des Geräts zahlen, da seine Einnahmen mit dem Gerät dann geringer sind. Die andere Variante: Illegal aufgestellte Automaten, die gar nicht angemeldet sind und sich meist in Hinterzimmern von Spielhallen befinden. »Die Betreiber solcher illegalen Geräte machen oft in wenigen Wochen Gewinne im sechsstelligen Bereich. Werden sie erwischt, müssen sie in der Regel die komplette Summe an das Finanzamt zahlen. Meine Aufgabe ist es unter anderem zu ermitteln, wie viel Umsatz mit einem Gerät erzielt wurde«, erklärt der Gutachter. Wie zum Beispiel bei einem automatischen Roulette-Tisch, der sechs bis acht Spielern gleichzeitig Platz bietet und illegal im Hinterzimmer einer Gaststätte aufgestellt war. Die anfallende Arbeit ist für eine Person allein nicht zu bewältigen, daher steht Michael Thelen seit Kurzem ein neuer Kollege zur Seite, der ihn dabei unterstützt. »Bei dem Job spielt auch Erfahrung eine wichtige Rolle – es kann daher durchaus drei Jahre dauern, bis sich der neue Kollege richtig in die Materie eingearbeitet hat«, so die Vermutung des Gutachters.

IMPRESSUM

Herausgeber
Ministerium für Inneres und Kommunales
des Landes Nordrhein-Westfalen
Friedrichstraße 62–80, 40217 Düsseldorf

Verantwortlich
Dieter Spalink,
Referat Öffentlichkeitsarbeit und
Online-Kommunikation

Redaktionsleitung
Ralf Hövelmann und Sonja Petrovic
Ministerium für Inneres und Kommunales NRW
Referat Presse- und Öffentlichkeitsarbeit
Redaktion *Streife*
Friedrichstraße 62–80, 40217 Düsseldorf
Tel. (0211) 871-23 66
Fax (0211) 871-23 44

CN-PolNRW 07-221-2366
Internet: www.streife.polizei.nrw.de
E-Mail: streife@mik.nrw.de
ISSN 0585-4202

Schlussredaktion
pressto GmbH, Köln

Autorinnen und Autoren dieser Ausgabe:
Katerina Breuer
Claudia Franken, LKA NRW
Kai-Uwe Kessen, LKA NRW
Nadja Kwasny, LKA NRW
Christian Mirgel, LKA NRW
Simone Wroblewski

Grafische Gestaltung und Satz
designiert Corporate Design, Düsseldorf

Druck
PHOENIX PRINT GmbH, Würzburg
Papier: Bright matt,
PEFC-zertifiziert

PEFC™
PEFC/04-31-1404
Förderung nachhaltiger Waldwirtschaft
www.pefc.de

Die *Streife* erscheint im Zwei-Monats-Rhythmus 6-mal im Jahr. Beiträge zur Veröffentlichung können direkt an die Redaktion gesandt werden.

Streife wird herausgegeben vom
Ministerium für Inneres und Kommunales des Landes
Nordrhein-Westfalen
www.streife.polizei.nrw.de /// ISSN: 0585-4202

POLIZEI
Nordrhein-Westfalen