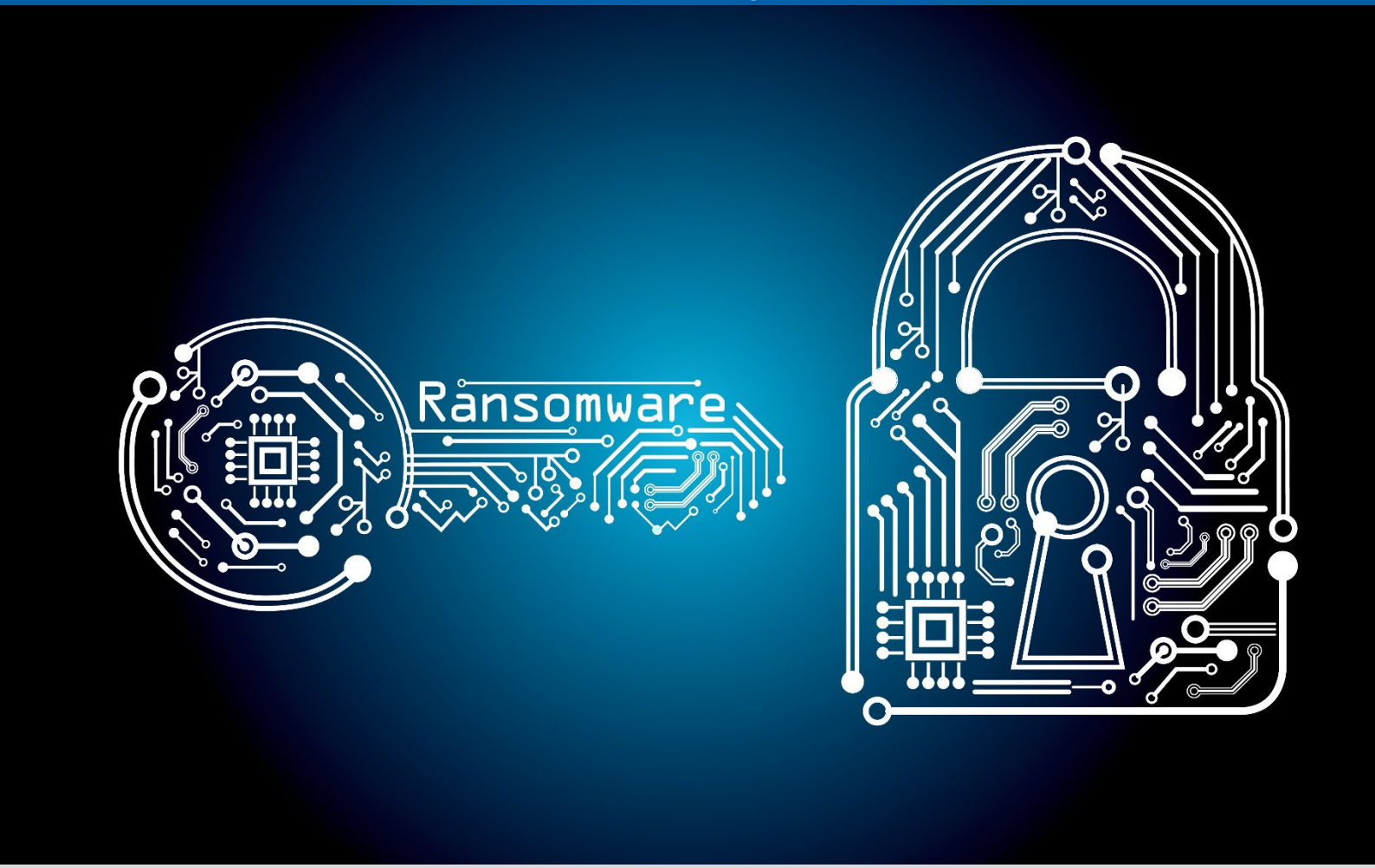
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert • professionell • rechtsstaatlich



Ransomware

Kurzinformation für Bürgerinnen und Bürger, Behörden und Unternehmen

Die zunehmende Digitalisierung in allen Lebensbereichen führt zu wachsenden Tatbegehungsmöglichkeiten für Cyberangriffe. Im Fokus der Angreifer stehen neben Wirtschaftsunternehmen auch öffentliche Institutionen, Behörden und Privatpersonen. Insbesondere Cyberangriffe mit Ransomware gehörten aktuell zu den gravierendsten Cyberbedrohungen. Durch Verschlüsselung ganzer IT-Systeme inklusive der Backups ergeben sich schwerwiegende Folgen für die Betroffenen. Cyberangriffe auf kritische Infrastrukturen (KRITIS) können zentrale Bestandteile des gesellschaftlichen Lebens gefährden.
Um die Gefahr einer Infektion mit Ransomware zu reduzieren, sollten geeignete Präventionsmaßnahmen zeitnah getroffen werden. Die nachfolgenden Präventionshinweise geben einen kurzen Überblick über wesentliche Basismaßnahmen.

Ransomware

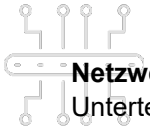
Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern. Häufig hinterlassen die Täter einen Hinweis, wonach eine Entschlüsselung der Daten gegen Zahlung eines hohen Lösegeldbetrags möglich sei. Zudem drohen sie bei Nichtzahlung mit der Veröffentlichung sensibler Daten, die sie zuvor heruntergeladen haben, um den Druck auf ihre Opfer zu erhöhen. Neben Kunden- oder Patientendaten können dies weitere für die Existenz eines Unternehmens kritischen Informationen sein.

Eine Infektion mit Ransomware erfolgt meist per E-Mail oder über eine Schwachstelle in Softwareanwendungen (Exploits). Häufig agieren Täter aus dem Ausland. Aufgrund unzureichender Kooperation einiger Staaten bei der Strafverfolgung, sind diese Täter für deutsche und europäische Strafverfolgungsbehörden nicht selten schwer oder nicht greifbar. Vor diesem Hintergrund sind präventive Maßnahmen die wesentliche Komponente, um unsere Gesellschaft vor diesen kriminellen Machenschaften zu schützen.

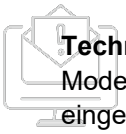
Präventionshinweise

Die dynamischen Entwicklungen im Bereich der Cybercrime stellen hohe Anforderungen an die Schutzmaßnahmen informationstechnischer Systeme, die fortlaufend angepasst werden müssen. Allgemeine Präventionsmaßnahmen bilden dabei die Basis zum Schutz vor Ransomware

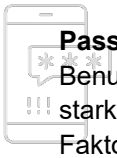
Softwareaktualisierungen
Sicherheitslücken durch inaktuelle Software sind offene Türen für Cyberangriffe. Daher ist es erforderlich Softwareanwendungen regelmäßig zu aktualisieren und nicht genutzte Dienste bzw. Softwareanwendungen zu deaktivieren oder zu löschen.



Netzwerksegmentierung
Unterteilen Sie Ihr Netzwerk in Zonen, die voneinander getrennt oder durch gesicherte Übergange geschützt sind. Eine Netzwerksegmentierung erhöht die Wahrscheinlichkeit, dass sich Schadsoftware nur in einem begrenzten Bereich ausbreiten kann und nicht Ihre komplette IT-Infrastruktur betroffen ist.



Technische Spam- und Malwarefilter
Moderne Spam- und Malwarefilter analysieren den eingehenden Mailverkehr. So können E-Mail-Postfächer zu einem gewissen Teil von E-Mails mit schadhaften Anhängen oder Spammails freigehalten werden.



Passwörter
Benutzeraccounts sollten grundsätzlich mit einem starken Passwort und sofern möglich mit einer 2-Faktor-Authentifizierung gesichert werden. Dies gilt insbesondere für Zugänge mit erweiterten Schreib- und Leserechten. Starke Passwörter haben insbesondere eine lange Zeichenfolge, die einen weiten Bereich der verfügbaren Zeichen ausnutzt.

Reduzierung privilegierter Zugänge
Privilegierte Zugänge (beispielsweise Admin Zugänge) mit besonderen Schreib- und Leserechten erhöhten die Gefahr einer Infektion mit Schadsoftware. Je weniger Nutzerinnen und Nutzer einen solchen Zugang besitzen, desto geringer ist das Risiko einer unbeabsichtigten Infektion mit Schadsoftware und einer Ausbreitung im Netzwerk.

Backups
Im Falle einer Verschlüsselung ermöglicht ein Backup eine Wiederherstellung der verschlüsselten Daten, vorausgesetzt das Backupkonzept ist auf seine Praxistauglichkeit und Recoveryfähigkeit getestet. Bei einem Ransomware-Angriff suchen die Angreifer mittlerweile gezielt nach vorhandenen Backups, um diese ebenfalls zu verschlüsseln. Daher ist es notwendig, die Dateien auch in Form eines Offline-Backups bzw. in einer geschützten Cloud zu sichern, um die Verfügbarkeit zu gewährleisten.

Firewall und Antivirensoftware
Eine leistungsstarke Next-Gen-Firewall mit implementierter Antivirensoftware hilft die IT-Infrastruktur auf unterschiedlichen Ebenen zu schützen. Moderne Firewalls überwachen u. a. den aus- und eingehenden Datenverkehr und prüfen Dateien auf Signaturen von Schadsoftware.

Mitarbeitersensibilisierung
Alle Beschäftigten müssen über die Gefahren durch Cyberangriffe regelmäßig informiert werden. Vorsicht gilt insbesondere beim Öffnen von E-Mail-Anhängen (auch bei bekannten Absendern) und beim Download von Dateien oder Plug-Ins aus dem Internet. Der Initialangriff vor der eigentlichen Verschlüsselung findet oft schon vorher statt. Angreifer kapern Firmenkommunikation, um durch Vortäuschen eines bekannten Absenders Beschäftigte zum Öffnen schadhafter E-Mail-Anhänge zu bewegen. Erfolgsversprechend ist eine umfangreiche Sensibilisierung aller Beschäftigten. Dabei können regelmäßige und professionelle Schulungen helfen.

Sie sind betroffen von einem Ransomware-Angriff?

Handeln Sie schnell!
Zur Begrenzung des möglichen Schadens sollten infizierte Systeme zunächst umgehend vom Netz getrennt werden.
Aktivieren Sie Ihre Notfallplanung, damit Ihre Mitarbeiter wissen, was zu tun ist und die entsprechenden Maßnahmen zur Schadensreduzierung unverzüglich eingeleitet werden.

IT-Sicherheitsdienstleister
Falls betroffene Unternehmen kein eigenes IT-Security Team / Computer Emergency Response Team (CERT) haben, welches den Vorfall bewältigen kann, sollte unmittelbar Kontakt zu zertifizierten IT-Sicherheitsdienstleistern hergestellt werden. Diese helfen bei einer Einschätzung des Schadensfalls und können dabei helfen, Ihre Daten wieder herzustellen. Eine Übersicht zertifizierter IT-Sicherheitsdienstleister finden Sie auf der Website des BSI. Die Leistungen dieser Dienstleister sind kostenpflichtig.

Nehmen Sie keine eigenständigen Entschlüsselungsversuche vor. Im allerschlimmsten Fall können Sie eine Entschlüsselung der Daten erschweren oder unmöglich machen.

Einspielen von Backups
Achtung: Schadsoftware könnte bereits seit Monaten auf Ihrem System aktiv und Backups entsprechend kontaminiert sein.

Zahlen Sie kein Lösegeld!
Jede Lösegeldzahlung bedeutet einen Taterfolg und sorgt dafür, dass die Täter weitere Straftaten begehen werden. Sie fördern durch die Zahlung von Lösegeldern die Weiterentwicklung und Verbreitung der Schadsoftware und es gibt keine Garantie, dass die Täter ihr Wort halten und Ihre Daten nach Zahlung entschlüsselt werden.

Erstatten Sie Anzeige!
Die Polizei kann Straftaten nur aufklären, wenn sie Kenntnis erhalten. Jede Erkenntnis kann dazu beitragen, Tat- oder Täterzusammenhänge zu erkennen und bestehende Präventions- und Bekämpfungsstrategien weiter zu verbessern.

Weiterführende Informationen zum Thema Ransomware und Cybersicherheit finden Sie hier

Bundesamt für Sicherheit in der Informationstechnik
Der Aufgabenbereich des BSI ist durch das „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ (BSI-Gesetz) festgelegt. Das BSI stellt u. a. Informationen zum Thema Cyber-Sicherheit in Form von Mindeststandards und Handlungsempfehlungen zur Verfügung, um Anwender bei der Abwehr von Cyber-Angriffen zu unterstützen.
www.bsi.bund.de

Projekt „No More Ransom“

Als Initiative der National High Tech Crime Unit der niederländischen Polizei, Europols europäischem Cybercrime Centers, Kaspersky und McAfee informiert das Projekt über die Funktionsweise von Ransomware und welche Maßnahmen umgesetzt werden können, um eine Infektion und damit eine Verschlüsselung zu verhindern.
www.nomoreransom.org

Koordinierungsstelle Cybersicherheit NRW
Mit der Einrichtung der Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen soll das Schutzniveau der Cybersicherheit in Nordrhein-Westfalen erhöht werden. Die Koordinierungsstelle bietet neben Informationen zum Thema Cybersicherheit auch einen Überblick über relevante Ansprechstellen und Initiativen.
www.cybersicherheit.nrw