Erstatten Sie Anzeige!
Die Polizei kann Straftaten nur aufklären, wenn sie Kenntnis erhält. Jede Erkenntnis kann dazu beitragen, Tat- oder Täterzusammenhänge zu erkennen und bestehende Präventions- und Bekämpfungsstrategien weiter zu verbessern. Darüber hinaus besteht die Möglichkeit, dass Angreifer durch zunehmenden Fahndungsdruck auch von weiteren Tatbegehungen absehen werden.

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.

Weiterführende Informationen

Bundesamt für Sicherheit in der Informationstechnik
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

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.

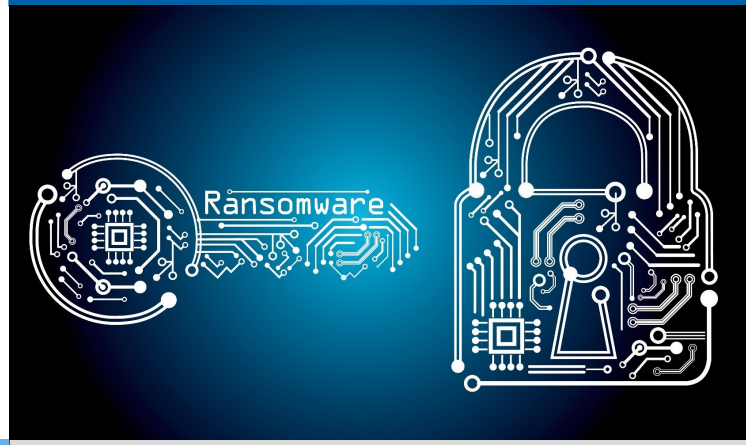
www.cybersicherheit.nrw

Herausgeber:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf
Telefon +49 211 939-0
E-Mail praevention.cybercrime.lka@polizei.nrw.de

Stand: 02/2022

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich



Ransomware
Kurzinformation für
Behörden und Unternehmen

lka.polizei.nrw

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 gravierensten Cyberbedrohungen. Cyberangriffe auf kritische Infrastrukturen (KRITIS) zeigen, dass Ransomware-Angriffe auch zentrale Bestandteile des gesellschaftlichen Lebens gefährden.

Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen gegen Zahlung eines Lösegeldes wieder freigeben. Eine Infektion mit Ransomware erfolgt meist per E-Mail oder über eine Schwachstelle in Softwareanwendungen (Exploits). Es gibt darüber hinaus weitere Möglichkeiten, durch die Schadsoftware ihren Weg zu informationstechnischen Systemen findet.

Präventionshinweise

Die dynamischen Entwicklungen im Bereich der Cybercrime stellen hohe Anforderungen an die Schutzmaßnahmen informationstechnischer Systeme, die zudem fortlaufend angepasst werden müssen. Bereiten Sie eine entsprechende Notfallplanung vor. Die nachfolgenden Maßnahmen sind lediglich ein Basisschutz.

Softwareaktualisierungen
Sicherheitslücken und veraltete Software sind offene Türen für Cyberangriffe. Daher ist es erforderlich, Softwareanwendungen regelmäßig zu aktualisieren und nicht genutzte Dienste bzw. Softwareanwendungen zu deaktivieren.

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

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

Passwörter
Nutzerzugänge sollten grundsätzlich mit starken Passwörtern und nach Möglichkeit mit einer 2-Faktor-Authentifizierung abgesichert sein. Dies gilt insbesondere für privilegierte Zugänge.

Reduzierung privilegierter Zugänge
Privilegierte Zugänge (beispielsweise Admin-Zugänge) mit besonderen Schreib- und Leserechten erhöhen 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.

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 unterstützt dabei, die IT-Infrastruktur mehrdimensional 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 aufgeklärt 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 und wiederkehrende Sensibilisierung aller Beschäftigten.

Sie sind betroffen? Handeln Sie schnell!

Aktivieren Sie Ihre Notfallplanung, damit Ihre Mitarbeiter wissen, was zu tun ist und die entsprechenden Maßnahmen zur Schadensreduzierung unverzüglich eingeleitet werden.

IT-Sicherheitsdienstleister
Stellen Sie unmittelbaren Kontakt zu zertifizierten IT-Sicherheitsdienstleistern her. 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. 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 sein und Backups entsprechend kontaminiert sein.