07 Air-Gap-Backups einsetzen

Backup-Systeme sind häufig ebenfalls im Fokus von Ransomware-Attacken. Sind diese erst einmal kompromittiert, sind sie für eine Wiederherstellung eines Systems unbrauchbar. Deshalb ist eine wirksame Backup-Strategie mit sog. Air Gaps erforderlich: Durch Isolierung der Speicherinfrastruktur vom internen Netzwerk und dem Internet kann ein Air-Gap-Backup offline erzeugt werden, wodurch Angreifer nicht mehr direkt auf diese Sicherungskopien zugreifen können. Dies erhöht im Schadensfall die Wahrscheinlichkeit, eine vollständige Wiederherstellung eines kompromittierten Systems zu erreichen.

lda.bayern.de/rp07

08 Netzwerkkomponenten up-to-date halten

Werden Sicherheitslücken in Softwareprodukten bekannt, dauert es nicht sehr lange, bis diese großflächig von kriminellen Ransomware-Gruppierungen ausgenutzt werden. Daher ist die Aktualität der Netzwerkkomponenten im kompletten Betrieb einer der wichtigsten Bausteine der Cybersicherheitsstrategie. Insbesondere Sicherheitsupdates für Firewalls oder VPN-Appliances müssen mit hoher Priorität zeitnah eingespielt werden, um Lücken schnell zu schließen. So wird das Zeitfenster für eine Cyberattacke über diesen Angriffsvektor auf ein Minimum reduziert.

lda.bayern.de/rp08

Cyberprävention
- mehr als nur ein Buzzword!

Ob Ransomware oder andere digitale Gefahren: Die fortlaufenden und immer komplexer werdenden Cyberangriffe sind bereits heute eine enorme Herausforderung für bayerische Betriebe. Hoffnungslos ausgeliefert ist man dieser Bedrohung allerdings auf keinen Fall. Gezielte Schutzmaßnahmen können davor bewahren, dass Hacker tief in Netzwerke vordringen, Daten stehlen und verschlüsseln. Frühzeitige Cyberprävention hat einen wesentlichen, positiven Einfluss darauf, ob und welcher Schaden bei einem Vorfall eintritt. Wer über den Basisschutz hinaus weitere Hindernisse für Angreifer aufbaut, macht es diesen besonders schwer und schützt nicht nur sich, sondern auch die Daten der betroffenen Personen. Das BayLDA stellt hierzu bayerischen Verantwortlichen aus dem nicht-öffentlichen Bereich Informationen über präventive Maßnahmen zum Schutz vor Cyberattacken zur Verfügung.

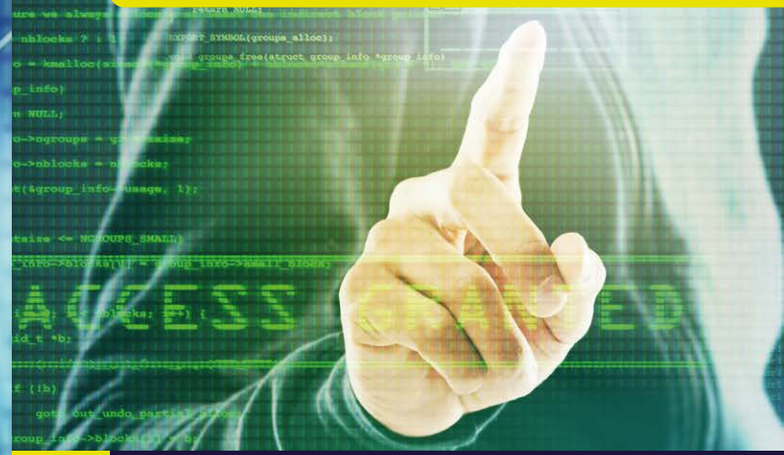
Cyberprävention
Mehr Sicherheit durch Datenschutz
www.lda.bayern.de

Herausgeber

Bayerisches Landesamt für Datenschutzaufsicht
Cybersicherheit und technischer Datenschutz
Promenade 18
91522 Ansbach

Bayerisches Landesamt für Datenschutzaufsicht

Cyberprävention
Mehr Sicherheit durch Datenschutz



8+

Ransomware ist auch nur Software
Acht Schutzmaßnahmen on top für ein Sicherheitsplus in der IT-Administration

01 Netzwerksegmentierung umsetzen

Um Cyberkriminellen das Bewegen und Ausbreiten innerhalb des Netzwerks (Lateral Movement) zu erschweren und effektiv davon abzuhalten, Daten organisationsweit zu verschlüsseln, ist eine Netzwerktrennung von Bereichen unterschiedlicher Kritikalität durch Firewalls in einzelne Subbereiche unersetzlich. So kann jedes einzelne Netzwerksegment mit individuellen Sicherheitsmechanismen ausgestattet und der Datenverkehr besser kontrolliert werden. Übersichtliche Netzwerksegmente helfen die Angriffsfläche für eine Ransomware-Attacke zu reduzieren.

lda.bayern.de/rp01

02 PowerShell begrenzen

Als mächtiges Werkzeug für Administratoren ist die PowerShell auch für Angreifer besonders attraktiv. Um das Missbrauchspotential des Tools einzuschränken, sind veraltete PowerShell-Versionen wie 2.0 zu deaktivieren, Fernzugriffe einzuschränken und Ausführungsrichtlinien für PowerShell-Skripte zu nutzen. Über Gruppenrichtlinien können diese verbindlich im gesamten Netzwerk angewendet werden. Auch gekaperte Administratoren-Accounts können daran gehindert werden, bösartige PowerShell-Skripte in Vorbereitung einer Verschlüsselung auszuführen.

lda.bayern.de/rp02

03 Programmausführung verhindern

Durch Application Whitelisting kann das Ausführen von unbekannten oder nicht genehmigten Programmen verhindert werden. Lediglich Anwendungen, die zuvor in einer Whitelist autorisiert wurden, können ausgeführt werden. Auch sollte durch Execution Directory Whitelisting geregelt werden, dass Programme nur aus festgelegten Verzeichnissen gestartet werden dürfen. So kann selbst Ransomware aufgrund fehlender Freigaben an einer Ausführung und Verbreitung gehindert werden.

lda.bayern.de/rp03

04 Fremde Office-Makros unterbinden

Ein weit verbreitetes Einfallstor für Ransomware-Attacken ist das Öffnen von per E-Mail versandten, manipulierten Office-Dateien mit Makros. Angreifer suggerieren dem Empfänger eine Dringlichkeit und liefern eine Anleitung mit, wie das enthaltene Makro aktiviert werden soll. Als präventive Schutzmaßnahme sollte das System zentral so konfiguriert werden, dass nur signierte Makros zugelassen werden und damit die Ausführung von Makros eingeschränkt wird. Bei Neuinstallationen und Updates von Office-Produkten sind die Einstellungen zu überprüfen und ggf. erneut anzupassen.

lda.bayern.de/rp04

05 Administrative Passwörter variieren

Administratoren besitzen mindestens zwei Nutzer-Accounts – einen für rein administrative Aufgaben und einen für normale Tätigkeiten rund um E-Mail und Internet. Für privilegierte Admin-Accounts sind ausschließlich starke Passwörter und Verfahren zur Zwei-Faktor-Authentifizierung zu wählen. Des Weiteren sind für lokale Admin-Kontos auf den einzelnen Clients individuelle Passwörter zuzuweisen. Mit dem Tool „Local Administrator Password Solution" können bspw. zufallsgenerierte Passwörter für lokale Admin-Kontos im Active Directory gespeichert werden.

lda.bayern.de/rp05

06 Internetübergang protokollieren und filtern

Mit einer Firewall wird üblicherweise der zentrale Internetübergangspunkt abgesichert und der http(s)-Verkehr über einen Web-Proxy geleitet. Dies ermöglicht eine restriktive Filterung für notwendige und erlaubte Zugriffe. Auffällige Zugriffsversuche und bekannte Indicators of Compromise können so gestoppt werden. Intrusion-Detection/Prevention-Systeme helfen, den Netzwerkverkehr auf schadhaftes Verhalten zu analysieren. Eine durchgängige Protokollierung für die Auswertung von Netzwerkaktivitäten (datenschutzrechtlich 60 bis 90 Tage vertretbar) lässt Cyberangriffe frühzeitig erkennen.

lda.bayern.de/rp06