04 | 24

Speicherverwaltung unter Exchange 2019

PowerShell-Skripte mit Task Scheduler planen

AD-Neuerungen in Windows Server 2025

ISSN 1614-2888
€ 14,80
Österreich € 17,00
Luxemburg € 17,00
Schweiz CHF 24,00

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Small-Business-IT

Passgenau

Server, Sicherheit und Strategien für KMU

Günstig und rechtssicher

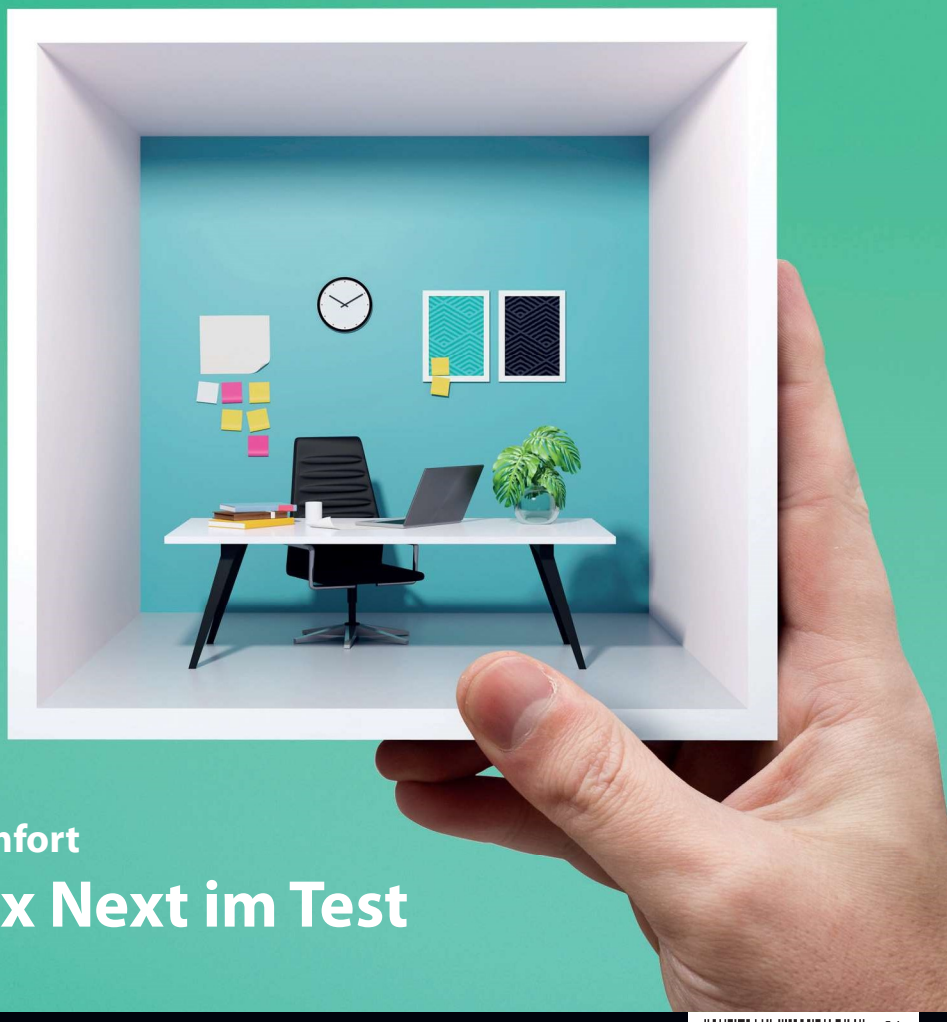
Windows und Office lizenzieren

Besseres Miteinander

Fileserver für Mac-Rechner mit Samba

Viel für wenig Geld

IT-Security für kleine Firmen



Kompakte Telefonanlage mit Komfort

Auerswald COMtrexx Next im Test

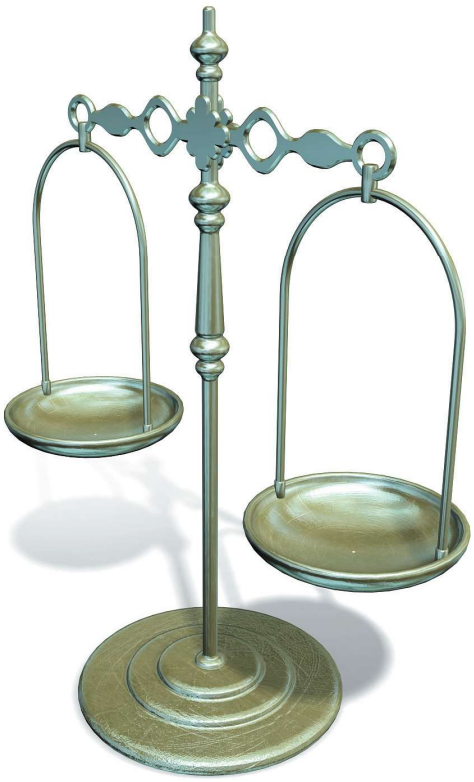
www.it-administrator.de

4 196583 214807 04

Cyberkriminelle nutzen gesetzliche Meldepflichten als Druckmittel

Boomerang

von Dr. Dennis-Kenji Kipker und Tilmann Dittrich



In unserer digital vernetzten Welt sind Cyberangriffe an der Tagesordnung. Doch damit nicht genug. Es gibt immer mehr gesetzliche Regularien zur Cybersicherheit. Und das machen sich zunehmend auch Cyberkriminelle zunutze, indem sie Cyberangriffe als erpresserisches Druckmittel einsetzen. Die rechtlichen Vorgaben, die eigentlich für mehr Sicherheit sorgen sollen, fliegen dann wie ein Boomerang zu den Opfern zurück.

Stellen Sie sich vor, Sie sind der CEO eines Unternehmens. In Ihrer Branche geht die Angst vor Cyberangriffen um. An einem Wochenende ruft Sie Ihre IT-Abteilung an und berichtet von Merkwürdigkeiten bei den IT-Systemen. Einige Stunden später geht gar nichts mehr, am Abend taucht ein Erpresserschreiben in einer Datei auf. Was jetzt? Wie kommt die Firma an die hohe geforderte Summe in Kryptowährungen? Ist denn nicht eigentlich eine Meldung an eine Behörde fällig? Dann fällt aber auf, dass jahrelang zu wenig für die IT-Sicherheit gemacht wurde. Und meinen es die Erpresser überhaupt ernst?

Druckmittel Meldung an Aufsichtsbehörde

Im November 2023 wurde ein Fall aus den USA bekannt, der belegt, dass bei dem geschilderten Fallbeispiel noch ein weiterer Gedankengang für die Leitungspersonen zu berücksichtigen ist: Dort war eine Ransomware-Gruppierung in die IT-Systeme eines Softwareunternehmens eingedrungen und hatte Daten exfiltriert, also für sich erbeutet. Die Kriminellen erpressten das Unternehmen mit einer Lösegeldforderung, die innerhalb von 24 Stunden zu begleichen war. Ansonsten sollte die Weitergabe der erbeuteten Daten stattfinden. Da das betroffene Unternehmen der Forderung nicht nachkam, aber die Kriminellen auch wussten, dass es seiner Meldepflicht gegenüber der Aufsichtsbehörde nicht innerhalb der gesetzlichen Frist nachgekommen war, informierten die Kriminellen kurzerhand die Behörde selbst über den erfolgreichen Angriff sowie die unterbliebene Meldung.

Erpressungsmöglichkeiten bei Cyberangriffen

Cyberkriminelle sind den Unternehmen oft einen Schritt voraus. Sie verändern ihre Angriffsarten sowie Erpressungsmuster stetig. Allseits bekannt ist die Erpressung aufgrund verschlüsselter Daten in den IT-Systemen, weil hierdurch die Betriebskontinuität der attackierten Einrichtung eingeschränkt wird. Hier locken die Kriminellen mit der Herausgabe von Wiederherstellungsschlüsseln. Eine weitere "Standard-Erpressungsmethode" stellt die Androhung der Veröffentlichung von erbeuteten Daten dar. Dabei kann es sich um kompromittierte Privatgeheimnisse (vor allem personenbezogene Daten), aber auch um Geschäftsgeheimnisse (etwa Kundenlisten, Forschungs- und Entwicklungsinformationen, Unternehmensstrategien) handeln.

Eine weitere Methode, mit der Cyberkriminelle ihre Opfer erpressen, ist die Androhung neuer oder eine Verschärfung bisheriger Angriffe. So warnte das Bundeskriminalamt bereits in seinem Cybercrime-Lagebild 2021 vor der Kombination von Ransomware- mit DDoS-Angriffen. Eine weitere Kombination eines stattgefundenen Angriffs stellt die Erpressung von Privatpersonen (in der Regel die von einer Datenschutzverletzung betroffenen Personen) sowie von Unternehmen innerhalb der Lieferkette dar. In seinem jüngsten Lagebericht zur IT-Sicherheit in Deutschland warnte das Bundesamt für Sicherheit in der Informationstechnik vor der Lukrativität von Supply-Chain-Angriffen aufgrund des Multiplikatoreffekts.

Es wird also deutlich, dass sich die Erpressungsmethoden stets in einem Wandel befinden. Ziel der Unternehmen muss es sein, die Vorgehensweise von Kriminellen zu verstehen und bestmöglich sogar zu antizipieren. Die Unternehmen müssen stets den Wert der von ihnen verarbeiteten Informationen evaluieren und dadurch vorhersehen können, ob Informationen aktuell besonders schützenswert sind.

Wir wollen dies an folgendem Beispiel verdeutlichen: Aufgrund des neuen Hinweisgeberschutzgesetzes ist ein Unternehmen verpflichtet, über seine interne Meldestelle Meldungen über Sachverhalte unter anderem zu strafbarem Handeln innerhalb des Unternehmens zu bearbeiten. Hierfür hat es von einem Dienstleister eine Software gekauft, hierbei allerdings übersehen, dass das Produkt keine gängigen Verschlüsselungsstandards berücksichtigt, ein Zugriff durch Dritte also leicht möglich ist.

Dieser Verstoß gegen das Hinweisgeberschutzgesetz, das für die Meldesysteme den Schutz der Vertraulichkeit verlangt,

könnte das Unternehmen zukünftig teuer zu stehen kommen. Denn die Cyberkriminellen könnten nun an äußerst sensible Informationen gelangen, die einen hohen Erpressungsdruck mit sich bringen. Diese Informationen sind nämlich pikant, können zu enormen Reputationsschäden führen und zuletzt drohen möglicherweise auch strafrechtliche Ermittlungen aufgrund der geleakten Informationen.

Meldepflichten im deutschen Recht

Das in den USA beobachtete Szenario ist auch auf deutsche Unternehmen übertragbar. Hier existieren mittlerweile einige gesetzliche Meldepflichten. Für wohl alle Unternehmen greifen die Vorschriften der Datenschutz-Grundverordnung (DSGVO). Kommt es hier zu einer Datenschutzverletzung, muss unverzüglich, spätestens binnen 72 Stunden nach Kenntnis über den Vorfall, eine Meldung an die zuständige Datenschutzaufsichtsbehörde erfolgen.

Eine neue Herausforderung kommt auf die Unternehmen zu, die kritische Dienstleistungen erbringen. Bislang existieren hier Vorgaben im BSIG für Kritische Infrastrukturen, Anbieter digitaler Dienste oder Unternehmen im besonderen öffentlichen Interesse. Spätestens bis Oktober 2024 muss eine EU-Richtlinie zur IT-Sicherheit umgesetzt sein, die den Anwendungsbereich des BSIG und auch die Meldepflicht bei Störungen signifikant verschärft.

Künftig ist die Meldepflicht im BSIG gestaffelt: Es müssen mindestens drei Meldungen (die erste unverzüglich, die letzte nach einem Monat) an das BSI abgegeben werden. Zusätzliche Meldezeitpunkte sind möglich. Weitere Meldepflichten gibt es im Energiesektor, im Telekommunikationsbereich, aber auch im Sozialrecht. Zudem gibt es auch noch Meldepflichten gegenüber Privaten.

Hierzu zählt natürlich die Benachrichtigungspflicht an die vom Datenschutzvorfall betroffenen Personen nach der DSGVO, aber vor allem auch die Anzeigepflicht gegenüber dem Versicherungsunternehmen im Rahmen einer Cyberversicherung ist von Bedeutung. Die Vertragsdokumente hierüber sind für die Cyberkriminellen Gold wert. Sie legen dar, ob mit (wahrscheinlichen) Lösegeldzahlungen zu rechnen ist, weil diese von der Versicherung abgedeckt sind. Sie bieten zudem aber auch Angriffspunkte für eine Verschärfung der Erpressung, weil für ein Unternehmen der Versicherungsschutz entfallen kann, wenn es der Anzeigepflicht aus dem Versicherungsvertrag nicht rechtzeitig nachkommt. Die Kriminellen können auch hier eine unterlassene Anzeige eines Cyberangriffs offenlegen.

Zudem besteht, wie das Beispiel der internen Meldestelle belegt, auch die Gefahr strafrechtlicher Ermittlungen, die die Kriminellen mit einer Weitergabe der erbeuteten Informationen an die Verfolgungsbehörden (oder über eine Veröffentlichung im Darknet) auslösen könnten.

Bußgeldsanktionen bei Meldepflichten

Der Fall aus den USA macht deutlich, dass die Meldepflichten stets innerhalb der Fristen vorzunehmen sind. Ein falsches Taktieren, um etwa Bußgelder aufgrund mangelhafter Sicherheitsmaßnahmen oder einen Reputationsschaden zu vermeiden, kann hier teuer werden. Denn die Meldepflichten sind regelmäßig an Bußgeldtatbestände geknüpft.

Längst ist bekannt, dass Verstöße gegen die DSGVO zu Millionenbußgeldern führen können. Auch in den anderen Rechtsvorschriften sind solche Bußgelder vorgesehen. Das Unternehmen will also nicht nur den Cyberkriminellen kein weiteres gefundenes Fressen liefern. Es muss vor allem verhindert werden, dass neue Anknüpfungspunkte für eine weitere Geldbuße gesetzt werden, wenn schon Sanktionen aufgrund unzureichender IT-Sicherheitsmaßnahmen zu befürchten sind.

Fazit

Cyberkriminelle verwenden gesetzliche Meldepflichten, die am Ende die IT-Sicherheit eigentlich verbessern sollen, gegen ihre Opfer. Dieser Artikel hat aufgezeigt, dass Unternehmen, die aus Kostengründen die IT-Sicherheit vernachlässigen, einem hohen Risiko ausgesetzt sind, Ziel eines Cyberangriffs zu werden. Diese Angriffe können nicht nur die Betriebskontinuität gefährden, sondern auch zu erheblichen finanziellen und Reputationsschäden führen.

Wichtig sind daher präventive Maßnahmen, die Vorbereitung auf den Ernstfall und das Einhalten gesetzlicher Meldepflichten. Unternehmen sind gefordert, behördliche Standards für IT-Sicherheitsmaßnahmen zu beachten, Notfallpläne zu erstellen und regelmäßig zu aktualisieren, die Zusammenarbeit zwischen IT- und Rechtsabteilungen zu stärken und den Ernstfall zu üben, um effektiv auf Cyberangriffe reagieren zu können. *(dr)* IT

Dr. Dennis-Kenji Kipker ist wissenschaftlicher Direktor des cyberintelligence.institute in Frankfurt am Main und Berater der Bundesregierung und der Europäischen Kommission in Fragen von Cybersicherheit und Technologieresilienz.

Tilmann Dittrich arbeitet als Rechtsreferendar im OLG-Bezirk Düsseldorf und ist Doktorand an der Heinrich-Heine-Universität Düsseldorf.

Handlungstipps für Unternehmen

1. Treffen Sie zumindest die gesetzlich vorgeschriebenen IT-Sicherheitsmaßnahmen. Hierfür ist eine Orientierung an behördlichen Standards möglich.
2. Bereiten Sie den Ernstfall vor: Ein Cyberincident-Plan kann nicht erst während eines Vorfalls erstellt werden.
3. Berücksichtigen Sie gesetzliche Meldepflichten in den Notfallplänen und sorgen Sie für die Zusammenarbeit von IT und Rechtsabteilung.
4. Üben Sie den Ernstfall: Awareness ist mehr als nur ein Modewort.
5. Ermitteln Sie bei IT-Vorfällen zeitnah und mit den notwendigen (gegebenenfalls auch externen) Ressourcen. Denken Sie hier immer auch an Fehlverhalten durch Unternehmensangehörige.
6. Geben Sie die Meldungen in den vorgesehenen Zeiträumen ab: Behörden und Versicherer können hier wichtige Hilfestellungen zur Krisenbewältigung geben. Zudem sind rasche Meldungen auch bei einem später festgestellten Fehlverhalten gegenüber der Behörde ein gutes Argument als Zeichen der Kooperation für die Entscheidung, ob und in welcher Höhe eine Sanktion in Betracht kommt.