IT-SICHERHEIT
Management und Technik

innovative VERWALTUNG

SPECIAL

IT-Sicherheit in der öffentlichen Verwaltung

Interview mit Markus Gringel von SECUDOS über Digitalisierung und IT-Sicherheit in öffentlichen Verwaltungen

„Man muss nicht immer das große Rad drehen."

Papierberge ade
Mit Digital-Workplace-Lösungen zu sicheren Prozessen

Managed-Security-Services
Wenn der Virenschutz an seine Grenzen kommt

Marktüberblick
Relevante Hersteller/Dienstleister und ihre Angebote

DATAKONTEXT

Zwischen Digitalisierung **und Cyberangriffen**

Mittlerweile hat man sich fast schon an die Meldungen über Cyberangriffe auf öffentliche Einrichtungen gewöhnt. Laut Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik sind zum Beispiel „die Regierungsnetze […] tagtäglich Angriffen aus dem Internet ausgesetzt. Neben überwiegend ungezielten Massenangriffen finden sich hierbei auch gezielte Angriffe auf die Bundesverwaltung." Aber nicht nur die Verwaltung selbst, sondern auch die IT-Dienstleister öffentlicher Einrichtungen geraten ins Visier von Kriminellen. So berichtete der Bayrische Rundfunk im Mai, dass Hacker IT-Firmen ausgespäht haben, die für Bundesministerien und Behörden arbeiten. Erbeutet wurden vermutlich große Mengen an E-Mail-Kommunikation mit personenbezogenen Daten und internen Informationen.

Neben der Aufgabe, sich vor Cyberattacken zu schützen, müssen öffentliche Einrichtungen derzeit die Digitalisierungsanforderungen stemmen, die das Onlinezugangsgesetz und das E-Government-Gesetz vorgeben. Das bedeutet aber auch, dass es in Zukunft noch mehr potenzielle Einfallstore für Hacker geben wird. Schon jetzt hinkt die öffentliche Verwaltung in Sachen IT-Sicherheit der Wirtschaft hinterher. So zeigt eine Studie zum Thema Softwaresicherheit beispielsweise, dass rund 82 Prozent der von Organisationen des öffentlichen Sektors entwickelten Anwendungen mindestens eine Sicherheitslücke aufweisen. Im Vergleich dazu waren es bei Privatunternehmen 74 Prozent. Die Ergebnisse basieren auf historischen Daten des Unternehmens Veracode und seiner Kunden.

Ein weiteres Problem ist der Fachkräftemangel. Hier muss der öffentliche Dienst mit der Wirtschaft konkurrieren – sowohl bei den Gehältern als auch bei den Arbeitsbedingungen. Es ist fraglich, ob sich Fachkräfte für Strukturen entscheiden, die oft starre Laufbahnen mit geringen Aufstiegschancen, unzureichenden Weiterbildungsmöglichkeiten und festen Gehaltsstrukturen bieten.

Insgesamt steht die öffentliche Verwaltung im Spannungsfeld zwischen Digitalisierungsdruck und Cybersicherheit noch vor großen Herausforderungen. Mit unserem Special „IT-Sicherheit in der öffentlichen Verwaltung" in Kooperation mit der Zeitschrift Innovative Verwaltung *können Sie sich einen Überblick über aktuelle Themen und praxisnahe Lösungen rund um das Thema Cybersicherheit verschaffen.*

Viel Spaß mit dem gemeinsamen Produkt!

Ihr
Sebastian Frank

Sebastian Frank

IMPRESSUM

IT-SICHERHEIT
Management und Technik

www.itsicherheit-online.com

in Kooperation mit

innovative VERWALTUNG

SPECIAL: IT-Sicherheit in der öffentlichen Verwaltung

Verlag:
DATAKONTEXT GmbH
Standort Frechen
Augustinusstr. 11 A · 50226 Frechen
www.datakontext.com

Chefredaktion:
Sebastian Frank (S.F.)
E-Mail: s.frank@kes.de

Online-Redaktion:
Jessica Herz (Leitung Online)
herz@datakontext.com
+49 2234 98949-80
Lisa Bieder
Konstantin Falke
Silvia Klüglich
Janek Mazac
Chiara Schönbrunn

Gründer: † Bernd Hentschel

Grafik/Layout/Satz:
Michael Paffenholz
Tel.: +49 173 8382572
E-Mail: michael.paffenholz@gmx.de
Objekt- und Anzeigenleitung:
Wolfgang Scharf
Tel.: +49 2234 98949-60
E-Mail: wolfgang.scharf@datakontext.com
zzt. gilt die Anzeigenpreisliste Nr. 29
Vertrieb/Herstellung:
Dieter Schulz
Tel.: +49 2234 98949-99
dieter.schulz@datakontext.com
Abonnement: Jahresabonnement € 129,- inkl. VK (Inland)

Erscheinungsweise: sechs Ausgaben
Alle Preise verstehen sich inkl. MwSt. Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.
Erscheinungsweise, Bezugspreise und -bedingungen: Abonnement und Bezugspreis beinhalten die Print-Ausgabe sowie eine Lizenz für das Online-Archiv. Die Bestandteile des Abonnements sind nicht einzeln kündbar. Der Preisanteil des Online-Archivs ist auf der Abonnementrechnung separat ausgewiesen.
Aboservice:
Hüthig Jehle Rehm GmbH, München,
Tel.: +49 89 21 83-7110
Druck: Grafisches Centrum Cuno GmbH & Co. KG, Calbe (Saale)

Genderhinweis: Gleichberechtigung ist uns wichtig! Für eine bessere Lesbarkeit unserer Fachtexte verzichten wir jedoch auf die gendergerechte Schreibweise und nutzen das generische Maskulinum als neutrale grammatikalische Form. Personenbezeichnungen beziehen sich auf alle Geschlechter.

Titelbild: SECUDOS GmbH
Fotos: Firmenbilder; DATAKONTEXT; 3dkombinat - stock.adobe.com, Deemerwha studio - stock.adobe.com, FourLeafLover - stock.adobe.com, golubovy - stock.adobe.com, Graficriver - stock.adobe.com, Gunel - stock.adobe.com, ii-graphics - stock.adobe.com, khunkorn - stock.adobe.com, Midnight Studio - stock.adobe.com, Nmedia - stock.adobe.com, rohman - stock.adobe.com, Studio Romantic - stock.adobe.com

29. Jahrgang 2023 · ISSN: 1868-5757

_Inhalt

2 Editorial

4 Mit Digital-Workplace-Lösungen den Arbeitsalltag optimieren
Papierberge ade, willkommen digitale Sicherheit!

6 Interview mit Markus Gringel, SECUDOS, über die Digitalisierung in öffentlichen Verwaltungen
„Man muss nicht immer das große Rad drehen."

8 Managed-Security-Services für die öffentliche Verwaltung
Wenn der Virenschutz an seine Grenzen kommt

10 Managed-Mail-Security für die öffentliche Verwaltung
E-Mail-Sicherheit den Profis überlassen

12 Reifegrad in Sachen Cybersicherheit ungenügend
6, setzen!

Anbieter

14 Sicherer Dateiaustausch in öffentlichen Einrichtungen
Digital-Workplace-Lösung als zuverlässige Arbeitskraft

16 **Mit Managed Endpoint Detection and Response die Cyberabwehr in die Hände von Security-Experten geben**

18 **E-Mail-Security für öffentliche Einrichtungen. Made in Germany.**

Mit Digital-Workplace-Lösungen den Arbeitsalltag optimieren

Papierberge ade, willkommen digitale Sicherheit!

Nahezu überall ist zu hören, dass wir mehr Ressourcen sparen müssen. Das gilt unter anderem auch für den Papierverbrauch. 2021 wurden in Deutschland insgesamt 19 Millionen Tonnen Papier, Pappe und Karton verbraucht – laut NABU sind das fast doppelt so viel wie vor zehn Jahren. Der Appell zur Ressourceneinsparung ist in der Wirtschaft und der Industrie bereits angekommen: Die meisten Unternehmen haben inzwischen ihre Arbeitsprozesse – auch bedingt durch die Corona-Pandemie – größtenteils digitalisiert. In öffentlichen Verwaltungen und Institutionen wird aber oft noch mit Papier gearbeitet, und es werden beispielsweise viele Dokumente per Fax oder Briefpost verschickt. Das vergrößert nicht nur den ökologischen Fußabdruck und entschleunigt die dringend benötige Digitalisierung, sondern schadet maßgeblich der IT-Sicherheit.

Öffentliche Einrichtungen, Kommunen und Verwaltungen verarbeiten täglich zahlreiche personenbezogene und sensible Daten – von Kraftfahrzeug- und Einwohnermeldeangelegenheiten, Gewerbe- und Wohngeldthemen bis zu Bauangelegenheiten. Gerade bei diesen Informationen ist ein mit der Datenschutzgrundverordnung (DSGVO) konformer Umgang und Versand essenziell, damit Unbefugte nicht darauf zugreifen können. Dies ist nicht nur für das Vertrauen der Bürger wichtig, sondern für Organisationen der kritischen Infrastruktur (KRITIS) auch verpflichtend. So müssen KRITIS-Betriebe besondere Sicherheitsauflagen erfüllen, die im IT-Sicherheitsgesetz festgehalten sind. Eine wesentliche Anforderung dabei: ein DSGVO-konformer Dateiaustausch.

Der Arbeitsalltag in öffentlichen Verwaltungen

Mitarbeiter in öffentlichen Verwaltungen haben ein vielseitiges Aufgabenfeld: Ein Teil der Mitarbeiter ist für die Bearbeitung von Anträgen zuständig, sei es für Ausweise, Pässe oder andere Dokumente. Sie prüfen Anträge auf Vollständigkeit und Richtigkeit, führen Datenbanken und halten Kontakt mit den Bürgern. Andere Mitarbeiter sind für die Buchhaltung, das Personalmanagement oder die Beschaffung von Materialien und Dienstleistungen verantwortlich. Sie führen administrative Aufgaben aus, wie zum Beispiel das Erstellen von Gehaltsabrechnungen oder die Überwachung von Bestellungen. Diese Aufteilung in verschiedene Bereiche führt dazu, dass regelmäßig verschiedene Dokumente ausgetauscht werden, da die Abteilungen auch übergreifend miteinander arbeiten müssen.

Darüber hinaus dienen öffentliche Verwaltungen für Bürger beispielsweise auch als Schnittstelle zu verschiedenen staatlichen Institutionen. So teilen die Mitarbeiter regelmäßig wichtige Dokumente mit Versicherungen oder Bauämtern, was heutzutage noch immer vorwiegend per Post oder Fax geschieht. Warum? Da die E-Mail die Mitarbeiter aufgrund der Größenbegrenzung beim Dateianhang spürbar einschränkt. Dass die Zuständigen dann stattdessen zu äußerst unsicheren Alternativen wie Brief oder Fax greifen, ist ihnen meistens nicht bewusst. Für eine spezielle IT-Sicherheitsschulung ist im Alltag oft keine Zeit.

Dateien versenden – digital und sicher

Beim Brief- oder Faxversand lässt sich niemals sicherstellen, dass die Nachricht ausschließlich nur den gewünschten Empfänger erreicht. Sensible Informationen können so schnell in falsche Hände geraten oder komplett verloren gehen. Das kann zu Rufschädigung und massiven Geldeinbußen führen.

Die Lösung: ein digitaler, sicherer Versand – und dabei ist nicht die Rede von E-Mails. Stattdessen bietet sich eine moderne Digital-Workplace-Lösung für den Arbeitsalltag an, wodurch jegliche Prozesse digitalisiert und optimiert werden können.

Optimierung des Arbeitsalltags

Mitarbeiter von öffentlichen Institutionen sind häufig an verschiedenen Orten, da sie entweder zwischen Homeoffice und Büro wechseln oder auswärtige Dienstreisen antreten. Daher ist es besonders wichtig, eine Lösung zu etablieren, die – anders als ein Faxgerät – von überall genutzt werden kann. Darüber hinaus lässt sich eine Digital-Workplace-Lösung optimal absichern: Die Nutzer können genau definieren, wer auf welche Dateien zugreifen darf. Dies ist zum Beispiel über die Vergabe eines Passworts möglich, das nur befugten Personen bekannt gegeben wird. Hinzu kommt, dass bei modernen Lösungen jeder Dateitransfer genau nachvollziehbar ist. So lässt sich jederzeit überprüfen, wann welche Datei mit wem geteilt wurde – Datenverlust ausgeschlossen. Zudem verschlüsseln DSGVO-konforme Lösungen die Dateien – sowohl während der Übermittlung als auch beim späteren Archivieren.

Aber Digital-Workplace-Lösungen optimieren nicht nur die Sicherheit in öffentlichen Verwaltungen. Sie reduzieren auch maßgeblich den ökologischen Fußabdruck und vereinfachen den Arbeitsalltag deutlich. So müssen beispielsweise Dokumente für den Versand nicht erst ausgedruckt werden, was Papier einspart und Zettelchaos auf Schreibtischen verhindert. Jedes Dokument befindet sich stattdessen auf der zentralen Austauschplattform und lässt sich darüber einfach und digital teilen – sowohl intern als auch extern. Ein Team-Transfer-Bereich ermöglicht es verschiedenen Personen, gemeinsam an Dokumenten zu arbeiten. So ist jeder Beteiligte immer auf aktuellem Stand, ohne dass Dateien ständig hin- und hergeschickt werden müssen. Arbeitsprozesse werden also deutlich beschleunigt. Die Größe der jeweiligen Datei ist dabei nicht von Bedeutung: Von einfachen Auftragsbestätigungen bis hin zu größeren Dateien wie Videoaufzeichnungen oder Grafiken – mit professionellen, digitalen Arbeitsplatzlösungen lassen sich Dateien jeder Größe und sogar komplette Ordnerstrukturen austauschen.

Neben dem Team-Transfer-Bereich erweist sich ist auch ein persönlicher Speicherplatz von Vorteil. Hat ein Mitarbeiter beispielsweise gerade einen Entwurf für eine Auftragsbestätigung erstellt, möchte darauf aber später noch einmal zurückgreifen, um diese vor dem Versand final zu überprüfen, kann er den Entwurf dort ablegen. Der Zugriff darauf ist für ihn dann jederzeit und von überall aus möglich.

Must-have einer Digital-Workplace-Lösung

Damit die Digital-Workplace-Lösung aber überhaupt den Arbeitsalltag in öffentlichen Verwaltungen optimieren kann, ist es wichtig, dass sie benutzerfreundlich ist und ohne großes Know-how eingesetzt werden kann. Eine geeignete Lösung lässt sich problemlos in die vorhandene Umgebung implementieren, beispielsweise über einen Desktop-Client oder als Outlook Add-In. Danach laufen alle wichtigen Funktionen im Hintergrund ab, ohne den Nutzer im Alltag zu stören. ■

Markus Gringel
ist Geschäftsführer von SECUDOS.

Interview mit Markus Gringel, SECUDOS, über die Digitalisierung in öffentlichen Verwaltungen

„Man muss nicht immer das große Rad drehen."

Ein sicherer Dateiaustausch ist unerlässlich – das gilt auch und gerade für öffentliche Verwaltungen. Aber wie können Mitarbeiter Dateien einfach, sicher und nachvollziehbar versenden? Die Antwort lautet: mit einer digitalen Arbeitsplatz-Lösung. Doch häufig ist die Digitalisierung in den Verwaltungen noch nicht angekommen. Wie ist der aktuelle Stand in den Behörden? Und mit welchen Hürden haben öffentliche Einrichtungen bei der Einführung von solchen digitalen Arbeitsplatz-Lösungen zu kämpfen? Darüber spricht Markus Gringel, Geschäftsführer von SECUDOS, im Interview.

IT-SICHERHEIT: Wie ist der aktuelle Stand der IT-Sicherheit in den Verwaltungen aus Ihrer Sicht, Herr Gringel?

Markus Gringel: Die Digitalisierung ist in vielen Verwaltungen noch nicht angekommen. In Behörden und Ämtern sind Faxgeräte nach wie vor gang und gäbe, um Dateien zu versenden. Doch das ist natürlich überhaupt nicht sicher und in Zeiten von Datenschutz nicht zu empfehlen. So ist nicht nachweisbar, ob die Dokumente angekommen sind. Aber viel wichtiger: Man weiß auch nicht, wer das Dokument erhalten hat. Denn bei einem Faxgerät kann jeder Mitarbeiter das Dokument aus dem Gerät entwenden. Damit können wichtige Unterlagen in die falschen Hände geraten oder sogar verloren gehen.

IT-SICHERHEIT: Welche Hürden stellen sich Ihrer Meinung nach den Verwaltungen? Was kann bei der Einführung einer digitalen Arbeitsplatz-Lösung schiefgehen?

Markus Gringel: Ich denke, die größte Hürde ist, dass viele Menschen davon überzeugt sind, dass man immer das große Rad drehen muss. Allerdings kann man schon mit punktuellen Lösungen die Digitalisierung vorantreiben. Jedoch ist die Internetverbindung häufig noch sehr schlecht, oder die PCs sind veraltet und gar nicht geeignet für eine digitale Lösung. Ein anderes Problem liegt oftmals darin, dass die Mitarbeiter die neuen Lösungen einfach nicht nutzen und lieber bei altbewährten Programmen bleiben. In vielen Fällen ist die Einarbeitung zu schwerfällig, die Lösung zu kompliziert, und nötige Schulungen für einen einfachen Einstieg fehlen.

IT-SICHERHEIT: Sie sprachen gerade von den Hürden, die es bei der Einführung von Arbeitsplatz-Lösungen zu überwinden gilt. Doch welchen Mehrwert können solche Lösungen den öffentlichen Einrichtungen bieten?

Markus Gringel: Digitale Arbeitsplatz-Lösungen können vor allem den Arbeitsalltag für die Mitarbeiter optimieren. Anders als beispielsweise Faxgeräte können sie von überall genutzt werden. Das bedeutet, dass die Mitarbeiter zwischen Büro oder Homeoffice wechseln, aber auch auf Dienstreise sein können und trotzdem Zugriff auf die Plattform haben. Bei vielen Lösungen gibt es auch persönliche Speicherplätze sowie Team-Transfer-Bereiche. Dort können Mitarbeiter dann gemeinsam an Projekten arbeiten oder sich mit Externen austauschen, ohne ständig Dateien hin- und herzuschicken. Das ist natürlich auch eine große Zeitersparnis für alle Beteiligten und beschleunigt die Arbeitsprozesse.

IT-SICHERHEIT: Aktuell herrscht Fachkräftemangel in vielen Branchen. Inwiefern wirkt sich das auf die IT-Sicherheit in Verwaltungen aus?

Markus Gringel: Der Fachkräftemangel ist natürlich aktuell ziemlich präsent. Das hat auch Folgen für die IT-Sicherheit in öffentlichen Verwaltungen. Wenn Personal fehlt, merken Unternehmen das häufig direkt. Fehlt dann auch noch Personal in einem so wichtigen Bereich wie der IT-Sicherheit, kann das schwerwiegende Konsequenzen haben. Werden die Systeme nicht ausreichend oder nicht kontinuierlich überwacht, weil schlichtweg nicht genug Leute dafür da sind, haben Hacker ein leichtes Spiel. Systeme können lahmgelegt oder auf wichtige und persönliche Daten kann unerlaubt zugegriffen werden. Das ist für öffentliche Verwaltungen natürlich das Worst-Case-Szenario. Umso wichtiger ist es, dass die Verwaltungen mehr Anreize schaffen, um Fachkräfte zu gewinnen und auch auf Dauer zu halten. ■

Sicheres Arbeiten mobil und im Home Office.

Mit der SINA Workstation sind sensible Daten premiumsicher.

Die SINA Workstation erfüllt als einzige Lösung standardmäßig alle BSI-Anforderungsprofile an einen sicheren Arbeitsplatz. VPN-Client, 2-Faktor-Authentisierung, Festplattenverschlüsselung und Schnittstellenkontrolle in einem Gerät.

secunet.com protecting digital infrastructures

secunet

Managed-Security-Services für die öffentliche Verwaltung

Wenn der Virenschutz an seine Grenzen kommt

Der Einsatz von Antivirensoftware ist in vielen Behörden und Verwaltungen Standard. Diese sind jedoch nur noch bedingt wirksam, da Cyberkriminelle heute häufig auf individualisierte und dateilose Angriffe setzen. Antivirenlösungen werden so oft umgangen. Zeit, um über andere Konzepte nachzudenken, zum Beispiel Managed EDR.

Cyberkriminelle setzen immer mehr auf neu entwickelte und komplexere Schadprogramme und ausgefeilte Angriffsmethoden, um ihre Ziele zu erreichen. Allein im vergangenen Jahr zählten die Security-Experten von G DATA fast 50 Millionen neue Samples. Im Vergleich zu 2021 ist das ein Anstieg von 107 Prozent. Oft verschaffen sich die Angreifer schon Monate bevor der eigentliche Angriff startet einen Zugang zum Netzwerk und spionieren es aus. Das gelingt besonders durch das Ausnutzen von Sicherheitslücken in Betriebssystemen oder Anwendungen. Erst zu einem späteren Zeitpunkt starten die Kriminellen ihre eigentliche Attacke, wie zum Beispiel die Verschlüsselung ganzer Systeme mit Ransomware.

Klassische Antivirenlösungen schützen vor Schadprogrammen und sind bewährte Komponenten einer Sicherheitsarchitektur. Sie verhindern damit sehr viele Cyberangriffe und deren fatale Folgen. Es gibt nur ein entscheidendes Problem: Sie kommen aufgrund der stetigen Weiterentwicklung von Malware und auch bei individualisierten Attacken schnell an ihre Grenzen. Cyberkriminelle setzen heute oft auf dateilose Angriffe, wohingegen klassische Virenschutzlösungen besonders für das Erkennen schädlicher Dateien ausgelegt sind. Die Angreifer nutzen beispielsweise Sicherheitslücken in Software und Betriebsprogrammen. Besonders problematisch ist das für öffentliche Einrichtungen, weil dort oft eine Fülle verschiedener Anwendungen im Einsatz ist, die immer auf aktuellem Stand gehalten werden müssen. Das ist eine große Herausforderung für die IT-Verantwortlichen, denn nur ein einziger erfolgreicher Angriff kann schnell die ganze Behörde oder Verwaltung arbeitsunfähig machen. Welche Möglichkeit gibt es aber, die IT-Systeme vor der Flut an Schadprogrammen zu schützen und zu verhindern, dass Cyberkriminelle ungestört das Netzwerk ausspionieren? Ein Ansatz ist Managed Endpoint Detection and Response (MEDR).

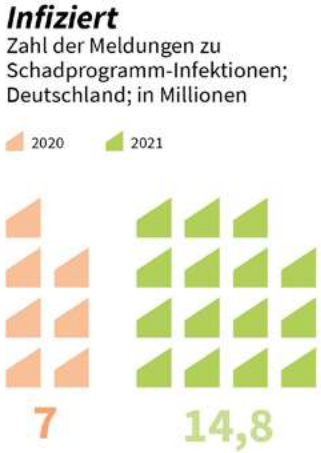


Abbildung 1: Zahl der Meldungen zu Schadprogramm-Infektionen in Deutschland (in Mio). (Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI); Aus: Cybersicherheit in Zahlen 2022/2023 | G DATA | Statista | brand eins)

Vorteile von MEDR gegenüber klassischem Virenschutz

Endpoint-Detection-and-Response-Lösungen sind sehr gut dafür geeignet, Angriffe zu entdecken, die klassische Antivirensoftware nicht erkennt. Das gelingt durch den Einsatz verschiedener Sensoren – besonders aus dem Bereich Verhaltenserkennung. Dabei wird auf den Endpoints geprüft, ob auffälliges Verhalten vorliegt, zum Beispiel das Ausführen nicht signierter Powershell-Scripts oder das Anlegen von Aufgaben mit erweiterten Nutzerrechten. Viele moderne Sicherheitslösungen bieten bereits Funktionen der Verhaltenserkennung, doch bei MEDR sind noch weitere Sensoren im Einsatz, die zum Beispiel Logfiles auf Endpoints auf Besonderheiten hin prüfen. Bei einer Managed-EDR-Lösung werden alle diese Vorgänge in Echtzeit durch Fachleute überwacht. Diese können einzelne Auffälligkeiten in Perspektive setzen, nach weiteren Indikatoren für schädliches Verhalten suchen und so ein fundiertes Urteil fällen, ob ein Angriff vorliegt oder nicht. Darüber hinaus erfolgt auf einen erkannten Angriff (Detection) unmittelbar eine Reaktion (Response), um diesen zu stoppen.

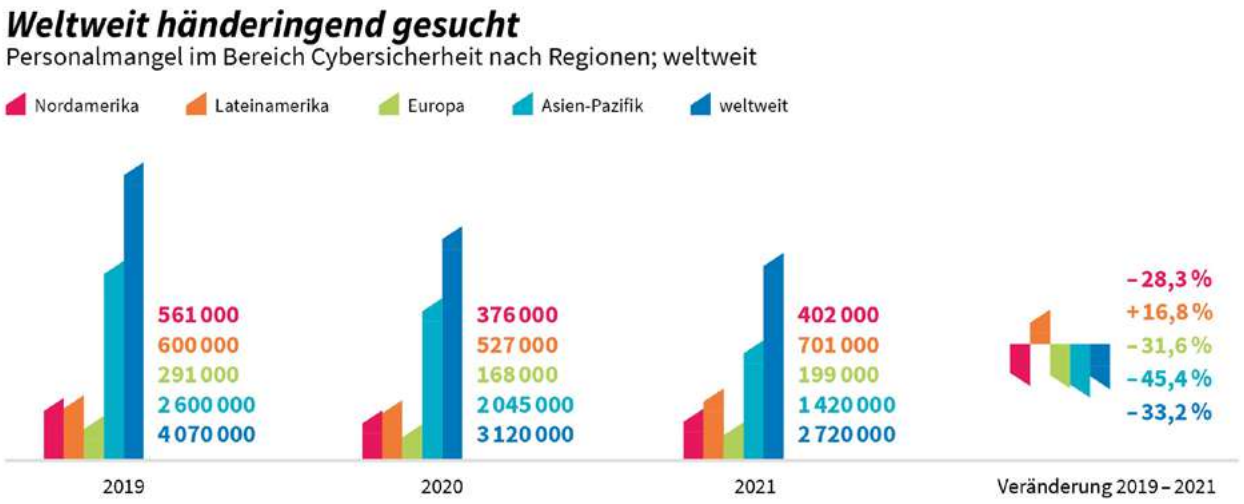


Abbildung 2: Im Jahr 2021 fehlten weltweit 2,72 Millionen Fachkräfte im Bereich Cybersicherheit. In Deutschland waren es 68 000. (Quelle: (ICS), Aus: Cybersicherheit in Zahlen 2022/2023 | G DATA | Statista | brand eins)

Diese Möglichkeit, sofort auf Ereignisse reagieren zu können, ist ein entscheidender Unterschied. Um potenziell schädliche Vorgänge zu analysieren und richtig einzuschätzen, ist ein hohes Maß an Expertise und Erfahrung bei den Analysten notwendig. Sie sind der wichtigste Bestandteil von Managed Endpoint Detection and Response. Sie prüfen verdächtige Ergebnisse, die aus der Sensorik stammen und reagieren sofort, wenn es nötig ist. Sie haben Zugriff auf alle relevanten Informationen, die erforderlich sind, um eine Entscheidung zu treffen, ob eine Aktion auf den Endpoints legitim ist oder nicht. Damit stoppen sie einen Cyberangriff bereits in der Anfangsphase, bevor dieser richtig startet, und verhindern weitreichende Schäden. Je nach Vorfall reagiert Managed EDR auch automatisiert, damit keine zusätzliche Zeit durch die manuelle Analyse verstreicht. Managed Endpoint Detection and Response ist dazu lernfähig. Durch Machine-Learning und die Erkenntnisse von manuellen Analysen trainiert sich die MEDR-Lösung, um Bedrohungen noch besser erkennen und stoppen zu können.

Behörden könnten auch versuchen, eigenes Personal einzustellen, um ihre IT-Systeme zu überwachen. Allerdings ist das oft unwirtschaftlich, da es sich um hochspezialisierte und erfahrene Fachleute handelt. Diese sind nicht nur teuer, sondern auch schwer zu finden. Sie haben häufig kein Interesse, in IT-Abteilungen zu arbeiten, in denen Cyberbedrohungen nur einen kleinen Teil des Aufgabenspektrums ausmachen. Es macht daher mehr Sinn, diese Aufgabe einem externen Anbieter anzuvertrauen.

Augen auf bei der Anbieterwahl

Entscheiden sich Behörden für einen Dienstleister, sollten sie darauf achten, dass dieser vertrauenswürdig ist. Dieser Punkt ist entscheidend, denn der Anbieter kümmert sich um die Sicherheit der IT-Infrastruktur und erhält detaillierte Einblicke in viele Bereiche. Wichtig ist auch, dass der Anbieter über langjährige Erfahrung in der IT-Sicherheit verfügt und auf diesen Bereich spezialisiert ist. Ein allgemeiner IT-Dienstleister ist wahrscheinlich keine gute Wahl, denn IT ist nicht gleich IT-Sicherheit. IT-Experten sind nicht zwangsläufig auch IT-Sicherheitsspezialisten. Nicht umsonst gibt es eigene Studiengänge an Fachhochschulen und Universitäten.

Zudem verfügt ein spezialisierter Security-Anbieter über wertvolle Erfahrungen aus Kundeneinsätzen, die auch bei Managed EDR wichtig für die Einschätzung von Vorfällen sein können, oder betreibt selbst Forschung in diesem Bereich. Auf internationaler Ebene finden regelmäßige Konferenzen und andere Möglichkeiten zum Austausch der Security-Spezialisten statt, um sich über neue Cybercrime-Strategien und Angriffsarten zu informieren. Kunden profitieren so von einer weitreichenden und fundierten Expertise ihres Dienstleisters. Ein weiterer entscheidender Punkt ist das Thema Support: Bei einem komplexen Thema wie der IT-Sicherheit ist es sinnvoll, einen Dienstleister zu wählen, der Support in der Landessprache anbietet und bei Problemen unkompliziert und verständlich unterstützt.

Fazit

Der Einsatz von Managed Endpoint Detection and Response ist für Behörden sehr sinnvoll, da ein klassischer Virenschutz schnell an seine Grenzen stößt. Managed EDR überwacht die IT-Systeme mit allen Vorgängen kontinuierlich und in Echtzeit und bietet einen weiteren, entscheidenden Vorteil: Durch die „Response"-Komponente lassen sich schädliche Aktionen im Zuge von Cyberangriffen sofort stoppen – ohne dass größere Schäden entstehen. Durch die Beauftragung eines externen Anbieters steigt nicht nur das Sicherheitsniveau, sondern die eigene IT-Abteilung hat dadurch auch mehr Zeit für andere Aufgaben und kann die Digitalisierung weiter vorantreiben.

Eine Managed-Endpoint-Detection-and-Response-Lösung gewährleistet ein hohes Schutzniveau, ohne dass hochspezialisiertes und teures Fachpersonal rekrutiert werden muss und ist daher auch wirtschaftlich eine gute Entscheidung. Es lohnt sich also für IT-Verantwortliche, über den Einsatz von Managed EDR nachzudenken. ■

Kathrin Beckert-Plewka
ist Public Relations Manager bei G DATA.

Managed-Mail-Security für die öffentliche Verwaltung

E-Mail-Sicherheit den Profis überlassen

Die öffentliche Verwaltung trägt im besonderen Maße Verantwortung für einen sicheren Umgang mit den Daten von Bürgerinnen und Bürgern. Mit der zunehmenden digitalen Kommunikation steigt auch die Gefahr von Missbrauch und Angriffen. Unser Fachartikel entstand in Zusammenarbeit mit einem kommunalen IT-Dienstleister und erläutert, warum viele Verwaltungen das Thema E-Mail-Sicherheit in die Hände externer Experten legen sollten.

Bei der E-Mail-Kommunikation sollten für die öffentliche Verwaltung Vertraulichkeit, Datenschutz und Sicherheit höchste Priorität haben. Der Verwaltung kommt ohne Frage eine Vorbildfunktion zu. Ein verantwortungsvoller Umgang mit den größtenteils sensiblen und personenbezogenen Daten sollte demnach selbstverständlich sein. Bürgerinnen, Bürger und Unternehmen müssen darauf vertrauen können, dass ihre Daten beim E-Mail-Verkehr sicher und geschützt sind.

Schließlich ist die sichere E-Mail-Kommunikation auch eine Frage der Compliance. Fünf Jahre nach Inkrafttreten der Datenschutzgrundverordnung (EU-DSGVO) muss die öffentliche Verwaltung sicherstellen, dass die Kommunikation mit den Bürgern den rechtlichen Anforderungen entspricht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt dabei klar die Inhaltsverschlüsselung und nicht nur die Transportverschlüsselung zwischen Kommunikationsknoten (TLS).

E-Mail-Kommunikation ist und bleibt Angriffsweg Nummer 1

Das Bundeskriminalamt (BKA) schildert in seinem Lagebild Cybercrime regelmäßig eindringlich, wie die öffentliche Verwaltung in Deutschland zunehmend Ziel für Cyber-Attacken ist. Auch in der öffentlichen Verwaltung gilt: Spam ist lästig, Phishing und Malware sind jedoch fatal. Ungesicherte E-Mail-Kommunikation ist nach wie vor eines der Haupteinfallstore für Malware. Ausgeklügelte Phishing-Attacken und Social-Engineering-Kampagnen versuchen, mit gefälschten E-Mails Zugangsdaten zu stehlen oder ungewollte Vorgänge auszulösen. Deshalb ist ein verlässlicher Schutz vor Spam, Malware, Phishing und Co. für die öffentliche Verwaltung zwingend notwendig.

Besondere Herausforderungen für die Verwaltung

Dabei zeigen sich drei besondere Herausforderungen für die öffentliche Verwaltung: Erstens sind die Kunden der öffentlichen Verwaltung die Gesamtheit aller Bürgerinnen und Bürger sowie Unternehmen und andere Organisationen im Land. Dementsprechend breit ist das Spektrum an Kommunikationspartnern via E-Mail mit Blick auf die Kompetenzen und Techniken in Sachen Mail-Security – von hochprofessionell bis völlig ahnungslos. Zudem ist das E-Mail-Aufkommen beachtlich. So verarbeitet beispielsweise ein IT-Dienstleister im kommunalen Umfeld aus NRW aktuell rund 70 000 externe E-Mails pro Tag für die angeschlossenen Kommunen und Einrichtungen – dabei ist der verwaltungsinterne E-Mail-Verkehr nicht mitgerechnet.

Diese Bandbreite und dieses Volumen trifft zweitens auf IT-Organisationen, die gerade erst einen drastischen Wandel hinter sich gebracht haben: Die pandemiebedingten Anforderungen an mobiles Arbeiten mit Homeoffice-Quoten von bis zu 95 Prozent haben zu einem drastischen Umbau der IT-Sicherheitsarchitektur vieler Verwaltungen geführt. Diesem Umbau unterlag zwar auch die Privatwirtschaft, doch war der Weg für viele Verwaltungen besonders weit. Zudem sind die IT-technischen Personalressourcen in der kommunalen Verwaltung ohnehin durch zahlreiche Digitalisierungsprojekte überlastet.

Drittens stehen Städte, Kreise und Gemeinden vor der Herausforderung, in dem dynamischen Umfeld der Cyber-Security Schritt zu halten. Die Angreifer werden zunehmend raffinierter und verwenden immer komplexere Techniken. Daher sind hoch qualifizierte Fachleute mit aktuellen Kenntnissen und Fähigkeiten unerlässlich. Sie sind auf dem Arbeitsmarkt kaum verfügbar und lassen sich – zumindest für kleinere Verwaltungen – inhouse wirtschaftlich nicht sinnvoll begründen.

Bild: Nmedia - stock.adobe.com

So sehen sich viele öffentliche Verwaltungen also mit dem Dilemma konfrontiert, als Angriffsziel besonders im Fokus zu stehen, jedoch nicht die notwendigen Mittel zur Abwehr parat zu haben.

Besser einen Service einkaufen als selbst zu scheitern

Vor diesem Hintergrund ist es für die meisten Verwaltungen sicher sinnvoll, die Sicherheit ihrer E-Mail-Infrastruktur in die Hände externer Spezialisten zu legen und sie als Managed-Mail-Security-Service einzukaufen. Tatsächlich planen laut einer Studie des Research-Unternehmens TechConsult aus dem letzten Jahr drei von fünf Verwaltungen genau dies zu tun.

Doch wie kann man ein solches Projekt angehen und worauf sollte man achten? Im Kern liegt der Erfolg in der richtigen Kombination aus Servicepartner und eingesetztem Produkt begründet.

Anforderungen an den Service-Provider

Der Service-Provider sollte eine langjährige Erfahrung im Betrieb von kommunalen IT-Infrastrukturen mitbringen. In der Regel sind zahlreiche Fachanwendungen mit der E-Mail-Lösung integriert und müssen entsprechend auch in der E-Mail-Sicherheit berücksichtigt werden. Zudem gibt es verwaltungsspezifische Mail- und Netzwerkdienste wie das besondere Behördenpostfach (beBPO) oder das verwaltungsinterne Bund-Länder-Kommunen-Verbindungsnetz NdB-VN, ehemals Deutschland-Online-Infrastruktur (DOI). Auch diese Dienste müssen effizient eingebunden und im Routing entsprechend genutzt werden können. Generell gilt, umso mehr Erfahrung der Service-Provider mit interkommunaler Zusammenarbeit hat, desto besser.

Durch etablierte Prozesse, die die Best Practices aus vielen verschiedenen Kundenszenarien abbilden, und einen 24/7-Support kann ein neuer Level an Qualität und Sicherheit erreicht werden. Wenn der Provider dann noch eine Private Cloud betreibt und BSI-zertifiziert ist, ist ein verlässlicher Partner gefunden. Service-Provider aus den Reihen der öffentlichen RZ-Anbieter haben zudem den Vorteil, dass sie eng in die verwaltungsinternen Meldestrecken von BSI, BKA und BND eingebunden sind und so früh wichtige Hintergrundinformationen zum Schutz der Verwaltungen bekommen können.

Auch das Produkt muss zur Verwaltung passen

Der zweite Erfolgsfaktor ist, dass die eingesetzte Technologie beziehungsweise das eingesetzte Produkt die notwendigen Eigenschaften und Funktionen mitbringt. Aus Technologiesicht bieten Gateway-basierte Lösungen hohe Benutzerfreundlichkeit und einen geringen Administrationsaufwand. Sie organisieren und implementieren den Schutz vor Angriffen sowie die Verschlüsselung von E-Mails an einer zentralisierten Stelle. Das bedeutet, dass der Endnutzer in der Regel nichts davon bemerkt und seine Arbeitsweise überhaupt nicht verändern muss. Allenfalls wird dem Nutzer per Outlook-Plug-In eine Auswahlmöglichkeit geboten und standardmäßig signiert und – wo möglich – verschlüsselt. Diese Benutzerfreundlichkeit erleichtert die Implementierung erheblich, da keine Mitarbeiterschulungen erforderlich sind und alle Konfigurationen zentral verwaltet werden. Verfügt die Lösung zudem über eine Selbstlernfähigkeit, passt sie sich kontinuierlich an variierende Kommunikationspartner und Umstände an.

Beim Schutz vor Spam, Phishing und Malware sollte das Produkt alle Register ziehen und viele Filter miteinander kombinieren können. Funktionen wie Content Disarming für verdächtige Anhänge oder URL-Safeguarding sind für die Verwaltung essenziell. Schön ist es zudem, wenn das Produkt über den Tellerrand von E-Mail-Security hinausschaut und ergänzende Funktionen wie beispielsweise einen Mechanismus zum Transfer großer Anhänge anbietet.

Wichtig ist auch eine vollständig automatisierbare Verwaltung von Zertifikaten, da sie für eine wirklich reibungslose Nutzung bei sehr geringem Administrationsaufwand sorgt. Als Managed-Service kann eine solche Lösung für E-Mail-Sicherheit und Verschlüsselung selbst für umfangreiche Verwaltungsstrukturen in nur wenigen Tagen eingeführt werden. Wenn das Produkt dann noch „made in Germany" ist und damit lokalen Compliance-Anforderungen entspricht, auf regionale Besonderheiten reagieren kann und mit einem leistungsstarken Support unterstützt wird, sollte dem Erfolg nichts im Wege stehen.

Dank Managed-Mail-Security ist heute guter Schutz und höchste Vertraulichkeit in der E-Mail-Kommunikation auch für kleine Verwaltungen mit engen Budgets gut und schnell umsetzbar. E-Mail-Sicherheit ist einfach, man muss es nur machen. ■

CHECKLISTE ANBIETERAUSWAHL

SERVICE-PROVIDER:

- viele Referenzen bezüglich kommunaler IT-Infrastruktur
- Erfahrung in interkommunaler Zusammenarbeit
- Integration mit genutzten Fachverfahren wird angeboten
- etablierte Prozesse und 24/7 Support
- eigene Private Cloud
- BSI-Zertifizierung

PRODUKTBASIS:

- Gateway-basiert
- selbstlernendes Whitelisting
- umfassender Spam-, Phishing- und Malware-Schutz
- starke Verschlüsselung nach Standards (PGP, SMIME)
- automatisierte Zertifikatsverwaltung
- regionale Anforderungen erfüllt (D, EU)

Stefan Cink
ist Business Unit Manager NoSpamProxy bei Net at Work GmbH.

Reifegrad in Sachen Cybersicherheit ungenügend

6, setzen!

Die Digitalisierung in der öffentlichen Verwaltung dauert zu lange, und es gibt Probleme im Bereich der Cybersicherheit. Das trifft auf eine deutlich gestiegene Bedrohungslage.

Das digitale Deutschland ist ein Failed State", bringt es Bitkom-Präsident Achim Berg auf den Punkt. „Das Onlinezugangsgesetz (OZG) zur Digitalisierung der Verwaltung in Bund und Ländern ist krachend gescheitert, und die Nachfolgeregelung eines OZG 2.0 verheißt keine wirkliche Besserung." Mit den geplanten Änderungen des Onlinezugangsgesetzes verpasse die Bundesregierung die Chance, die Digitalisierung der Verwaltung wirklich konsequent voranzutreiben. „Der Bund will sich noch einmal fünf Jahre Zeit lassen, bis seine eigenen Verwaltungsleistungen digital abgewickelt werden können", so Berg weiter.

Aber nicht nur die Digitalisierung insgesamt ist problematisch, auch im Bereich der Cybersicherheit haben vor allem die Kommunen ihre Hausaufgaben nicht gemacht. So fasste Dr. Gehard Schabhüser Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in einer Rede auf dem BSI-Kongress die Situation wie folgt zusammen: „Die Lage der IT-Sicherheit in Deutschland ist angespannt, dynamisch und vielfältig – und damit so hoch wie noch nie. Die zentrale Schlussfolgerung ist: Wir müssen eine Steigerung der Cyber-Resilienz unserer IT-Systeme erreichen." Über die NIS-2-Richtlinie der EU würden auch die Verwaltungen mehr in die Pflicht genommen: „Das ist sicherlich ein vernünftiger Schritt." Hinsichtlich der NIS-2-Umsetzung plädierte Schabhüser für gleichlautende Landesgesetze sowie eine Mitregulierung des kommunalen Sektors, da gerade dort besonders viele Leistungen für Bürger erbracht werden und leider gleichzeitig noch kein hoher Reifegrad in Sachen Cybersicherheit zu beobachten sei.

Zaghafte Regulierung und Fachkräftemangel

Dass die öffentliche Verwaltung durch NIS-2 stärker in die Pflicht genommen wird, sieht Dennis-Kenji Kipker, Professor für IT-Sicherheitsrecht an der Hochschule Bremen, nicht ganz so. In der Zeitschrift <kes> schreibt er dazu: Es „fällt jedoch auch bei NIS-2 weiterhin auf, dass einem strengen Umgang mit privatwirtschaftlichen Anbietern ein eher zaghafter Ansatz zur Regulierung des öffentlichen Sektors gegenübersteht – obwohl sich gerade dort in der Vergangenheit regelmäßig erhebliche Schwächen der Cybersicherheitspraxis gezeigt haben und nach wie vor zeigen." Die NIS-2-Regelungen für die Cybersicherheit des öffentlichen Sektors seien nicht ausreichend.

Darüber hinaus verschärft der Mangel an qualifiziertem Personal die Probleme der öffentlichen Verwaltung bei der Umsetzung von Sicherheitsstandards. Bereits 2021 fehlten weltweit 2,72 Millionen Fachleute im Bereich Cybersicherheit (siehe auch S. 43). Besonders betroffen ist der öffentliche Dienst, denn hier treffen laut einer Analyse der Stiftung Neue Verantwortung die High-Potentials auf starre Gehaltsstrukturen, ein hierarchisch organisiertes Laufbahnrecht, die Bevorzugung von Generalisten und Juristen, traditionelle Arbeitsformen in nicht-interdisziplinaren Teams und auf fehlende Weiterbildungsmöglichkeiten.

Hilfe naht

Aber es gibt auch Hilfsangebote für Behörden und Ämter. Zum Beispiel erprobt das BSI seit Mai zusammen mit sechs deutschen Modellkommunen das Pilotprojekt „Weg in die Basis-Absicherung" (WiBA). Laut BSI-Vizepräsident Schabhüser sei besonders für kleinere Kommunen die Umsetzung der IT-Grundschutz-Standards des BSI zu komplex. „Für diese Kommunen bieten wir mit WiBA eine neue Einstiegsebene in den IT-Grundschutz an: Wir versorgen sie mit Checklisten, Prüffragen und Hilfsmitteln, mit denen sie die dringlichsten Maßnahmen selbst identifizieren und umsetzen können", so Schabhüser weiter.

Die Dringlichkeit des Fachkräftemangels wurde auf EU-Ebene erkannt: Die EU-Kommission hat im Rahmen des „Europäischen Jahres der Kompetenzen 2023" eine Akademie für Cybersicherheitskompetenzen vorgestellt, um ein besser koordiniertes Vorgehen zur Schließung der Fachkräftelücke im Bereich der Cybersicherheit zu erreichen. Die Akademie wird verschiedene bestehende Initiativen zur Förderung von Cybersicherheitskompetenzen auf einer Online-Plattform zusammenführen, um sie so besser sichtbar zu machen und die Zahl qualifizierter Cybersicherheitsfachkräfte in der EU zu erhöhen (https://digital-skills-jobs.europa.eu/). Inwieweit diese Maßnahme dem Fachkräftemangel entgegenwirken kann, wird sich zeigen. ■

S.F.

HFCON

Human Firewall Conference 2023

powered by sosafe

16.–17. November 2023

BALLONI Hallen, Köln

(ISC)² Sammeln Sie CPE-Credits!

Bei dieser Security-Konferenz dreht sich alles um eines: **den Faktor Mensch**

Lernen Sie von Expertinnen und Experten, tauschen Sie sich mit anderen Security-Verantwortlichen aus und erweitern Sie Ihren Blickwinkel um innovative Ansätze.

mit Speakern **Ulrich Irnich, Sascha Lobo, Jamie Bartlett, Inge van der Beijl** und vielen mehr!

Jetzt kostenloses Ticket sichern!

Sicherer Dateiaustausch in öffentlichen Einrichtungen

Digital-Workplace-Lösung als zuverlässige Arbeitskraft

Der Personalausweis ist abgelaufen, der Führerschein muss neu ausgestellt werden, die Eheschließung angemeldet oder der Wohnsitz umgemeldet werden – all diese Aufgaben haben eines gemeinsam: Sie enden mit einem Besuch in einer öffentlichen Einrichtung oder Verwaltung. Tagtäglich werden dort personenbezogene Daten verarbeitet. Insbesondere diese Daten gilt es, DS-GVO-konform zu versenden. Viele Einrichtungen setzen dabei nach wie vor auf das Faxgerät. Papierloses Büro – Fehlanzeige! Gelangen die Daten jedoch in falsche Hände, kann das Konsequenzen haben. Aus diesem Grund bietet sich die digitale Arbeitsplatzlösung Qiata an, mit der Dateien einfach, sicher und nachvollziehbar versendet werden können.

KRITIS-Unternehmen müssen hohe Sicherheitsanforderungen erfüllen, wenn es um das Verarbeiten und die Übermittlung von Daten geht. Grund dafür ist das IT-Sicherheitsgesetz, das vorschreibt, dass die sichere Datenverarbeitung gewährleistet sein muss. Dies macht einen DS-GVO-konformen Austausch unabdingbar. Doch die Nutzung von Faxgeräten ist mittlerweile längst nicht mehr sicher und auch veraltet. Eine digitale Lösung kann dabei helfen, die Arbeit zu vereinfachen und Informationen schnell und sicher auszutauschen – intern, aber auch extern.

Qiata: einfach, sicher und nachvollziehbar

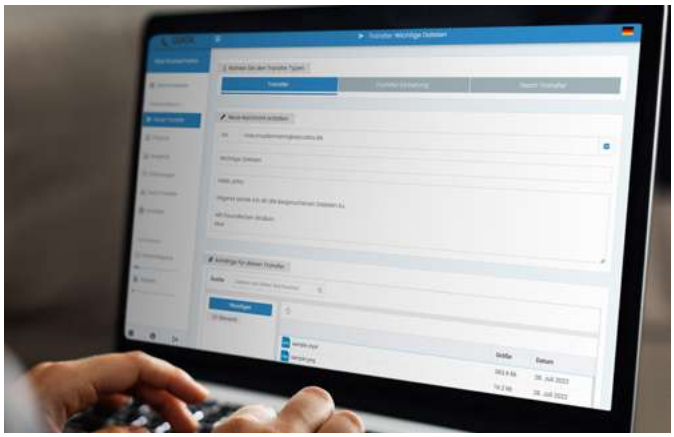
Sucht man eine solche Digital-Workplace-Lösung, ist man bei Qiata vom deutschen Lösungsanbieter SECUDOS genau richtig. Mit Qiata können Dateien einfach, sicher und nachvollziehbar ausgetauscht werden. Verschiedene Dateitypen oder auch ganze Ordnerstrukturen lassen sich per Outlook Add-in, über den Desktopclient oder die Weboberfläche versenden. Dabei spielt es auch keine Rolle, welche Größe die zu versendenden Dateien haben.

Setzen öffentliche Einrichtungen, Kommunen oder Verwaltungen Qiata ein, erleichtern sie auch den Bürgern den Alltag: Unterlagen müssen nicht mehr per Post verschickt oder persönlich vorbeigebracht werden. Sie können den Mitarbeitern ganz einfach über das Tool zur Verfügung gestellt werden. Hierzu wird lediglich eine E-Mail-Adresse des Empfängers benötigt.

Arbeitserleichterung im Alltag

Qiata eignet sich aber nicht nur für den internen Dateiaustausch, auch extern lassen sich Dateien versenden oder empfangen. Wenn Behörden beispielsweise Daten mit dem Finanzamt austauschen müssen, ist das dank der Filetransfer-Plattform kein Problem. Durch den TeamTransfer-Bereich können darüber hinaus Dokumente gemeinsam bearbeitet werden. Der persönliche Bereich von Qiata ermöglicht das Abspeichern von Informationen, auf die der Mitarbeiter jederzeit und überall zugreifen kann. Daraus ergeben sich zwei große Vorteile: die Optimierung der Arbeitsabläufe und ein effizienteres Arbeiten. Zudem bleiben Einrichtungen dank der Digital-Workplace-Lösung stets Herr über ihre Daten.

Mehr dazu hier



Vorteile von Qiata für öffentliche Einrichtungen:

- ✓ Veraltete und unsichere Prozesse wie Fax und Brief werden digitalisiert.
- ✓ Der Papierverbrauch wird reduziert, was sich positiv auf den ökologischen Fußabdruck auswirkt.
- ✓ Auch im Homeoffice können die Mitarbeiter jederzeit sicher Dateien verschicken.
- ✓ Es ist kein technisches Know-how notwendig – mit wenigen Klicks lassen sich Dokumente von überall aus über die Weboberfläche, den SECUDOS Desktop Client (SDC) oder das Outlook Add-in übermitteln.
- ✓ Die Datenbewegungen sind eindeutig nachvollziehbar – Daten können also nicht verloren gehen oder verschwinden.
- ✓ Es wird gewährleistet, dass die zu versendenden Dateien auch wirklich beim gewünschten Empfänger ankommen.
- ✓ Alle Daten sind durch die 256-Bit-AES-Verschlüsselung sowohl während des Versands als auch bei der anschließenden Archivierung sicher. Vorab kann genau definiert werden, wer Zugriff hat.
- ✓ Die Richtlinien der Datenschutz-Grundverordnung (DS-GVO) werden eingehalten. Das Auskunftsrecht, das Recht auf Berichtigung, die Datensäuberung und -übertragung sind mit Qiata gesetzeskonform umsetzbar.
- ✓ Die Appliance hilft, den Arbeitsalltag zu vereinfachen und die Vielzahl von Dokumenten den Griff zu bekommen.

QIATA

procilon GROUP

proGOV

Sichere Lösungen für Verwaltungen

XTA

Sichere Behördenkommunikation

✓ XTA – für sicheren Datenaustausch in XÖV-fähigen Fachanwendungen
✓ XTA2 – der Lösungsbaustein für standardisierte Transportverfahren

beBPo

Sichere Justizkommunikation

✓ „ERV so einfach wie E-Mail“ im vorhandenen Mail-Client anwenden
✓ Austausch: andere Behörden, Anwälte, Notare & Verfahrensbeteiligte

TR-ESOR

Sichere Aufbewahrung

✓ Elektronische Dokumente gerichtsfest aufbewahren
✓ Einfache Erweiterung vorhandener Dokumentenmanagement-Systeme

Mail-connect

Sichere Bürgerkommunikation

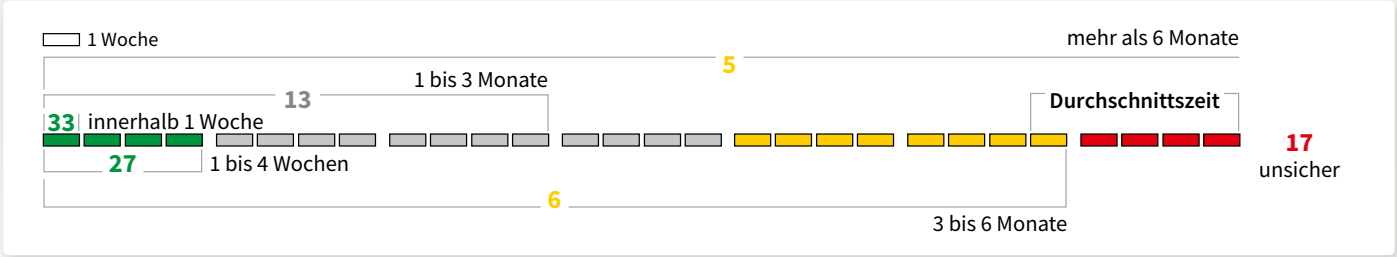
✓ Datenschutzkonforme Übermittlung zwischen Behörden und Bürgern
✓ Automatische Zustellung über eine für Bürger kostenfreie Sicherheitsplattform

anfrage@procilon.de | +49 34298 4878 31 | www.procilon.de

Mit Managed Endpoint Detection and Response die Cyberabwehr in die Hände von Security-Experten geben

Effektive IT-Sicherheit ist aufwendig, kompliziert und erfordert viel Know-how sowie spezielles Fachpersonal. Öffentliche Verwaltungen stellt die Abwehr von Cybergefahren oft vor große Herausforderungen. Sie sind mit der Digitalisierung ihrer Strukturen und Prozesse voll ausgelastet. Für IT-Sicherheit bleiben oft keine Ressourcen übrig. Zudem fehlt es an Personal und dadurch auch am nötigen Fachwissen. Wie aber kann man unter diesen Bedingungen die IT-Systeme effektiv und umfassend gegen Cyberangriffe absichern? Die Antwort lautet: Mithilfe von G DATA 365 Managed Endpoint Detection and Response (MEDR).

Lange Leitungen



Zeit, die vergeht, bis Sicherheitsvorfälle entdeckt werden; ausgewählte Regionen*; Entscheiderinnen und Entscheider im Bereich IT- und Unternehmenssicherheit; 2021; in Prozent.

Nordamerika 57 %, APAC (Wirtschaftsraum Asien Pazifik) 35 %, EMEA (Wirtschaftsraum Europa, Naher Osten und Afrika) 17 %. (Quelle: Foundry)

IT-Sicherheit ist eine Rund-um-die-Uhr-Aufgabe, denn Cyberkriminelle sind nicht nur tagsüber, sondern vor allem auch nachts, an Feiertagen und am Wochenende aktiv. Zudem setzen die Angreifer heute vermehrt auf dateilose und gezielte Angriffe, die oft monatelang laufen und nicht entdeckt werden. Die IT-Systeme müssen daher immer im Auge behalten werden, und im Fall einer Attacke muss eine sofortige Reaktion erfolgen, um große Schäden abzuwenden. Dies können öffentliche Verwaltungen häufig kaum leisten. Eine Lösung ist Managed EDR von G DATA CyberDefense. Dabei überwachen gut ausgebildete IT-Security-Spezialisten alle Aktivitäten auf den IT-Systemen und stoppen Cyberangriffe – egal zu welcher Uhrzeit. Behörden können sich zudem auf die effektiven Security-Technologien und eine erweiterte Threat-Detection-Sensorik „made in Germany" verlassen.

24/7-Expertenschutz

Das Monitoring übernimmt bei G DATA 365 Managed Endpoint Detection and Response ein Team von erfahrenen Analyst*innen. Sie sind dabei 24 Stunden täglich und an sieben Tagen in der Woche im Einsatz und werten die Ergebnisse der Sensorik aus. Dabei verifizieren sie zunächst, ob es sich um eine Attacke handelt. Ist dies der Fall, wird der Angriff genauestens analysiert. Danach erfolgen eine umgehende Reaktion sowie eine Einleitung von Gegenmaßnahmen, wie zum Beispiel die Separierung eines betroffenen Endpoints oder Dienstes vom Netzwerk. Kund*innen werden zudem über den Vorfall informiert, in dringenden Fällen auch per Anruf. Sollte eine Mitwirkung durch die eigene IT-Abteilung nötig sein, geben die Expert*innen von G DATA klare Handlungsempfehlungen.

Alle Informationen laufen in der Webkonsole zusammen, in der IT-Teams in Echtzeit eine Übersicht darüber erhalten, ob und welche Security-Vorfälle es gab und welche Maßnahmen die Analyst*innen von G DATA ergriffen haben. Zudem finden sie hier Handlungsempfehlungen, wenn diese nötig sind.

Öffentliche Verwaltungen profitieren beim Einsatz der gemanagten EDR-Lösung von der langjährigen Erfahrung und dem Know-how des deutschen Cyber-Defense-Spezialisten. Mitarbeitende in Behörden können sich voll und ganz ihren Aufgaben widmen, während G DATA die IT-Systeme überwacht und Angriffsversuche stoppt. Der Cyber-Defense-Spezialist hat zudem alle Komponenten seiner Managed-EDR-Lösung selbst entwickelt, sodass die Analyst*innen Vorgänge im Netzwerk auch sicher deuten können. Der deutschsprachige und kostenfreie 24/7-Support unterstützt Behörden bei Fragen und Problemen. Dadurch müssen IT-Verantwortliche nicht in zusätzliche Fachkräfte investieren, die sonst nötig wären, um die IT-Sicherheit zu gewährleisten. Ein weiterer Vorzug der Dienstleistung: Die verarbeiteten Daten verbleiben ausschließlich in Deutschland auf den Servern des strategischen Partners IONOS in Frankfurt am Main und Berlin sowie auf den unternehmenseigenen Servern von G DATA am Bochumer Unternehmensstandort. Damit unterliegen die Informationen den strengen deutschen Datenschutzgesetzen und der EU-Datenschutz-Grundverordnung. ■

Sie möchten weitere Informationen zu G DATA 365 Managed Endpoint Detection and Response und haben Interesse an einer kostenfreien Live-Demo? Dann besuchen Sie unsere Webseite

www.gdata.de/medr

Kontaktinformationen:
G DATA CyberDefense AG
Königsallee 178
44799 Bochum
Deutschland
Telefon: +49 (0) 234 / 97 62-0
Telefax: +49 (0) 234 / 97 62-299
E-Mail: info@gdata.de

Mehr dazu hier

G DATA CyberDefense

E-Mail-Security für öffentliche Einrichtungen. Made in Germany.

Immer mehr öffentliche Einrichtungen werden zum Ziel von Cyberangriffen. Mit dem starken Spamschutz und der sicheren E-Mail-Verschlüsselung von NoSpamProxy schützen Sie sich und die Daten von Einwohnenden und Mitarbeitenden.

Öffentliche Einrichtungen der Verwaltung und des Gesundheitswesens stehen besonders im Fokus von Cyberkriminellen. Sie sind als Schlüsselstellen für das Funktionieren des Gemeinwohls als Angriffsziel leider besonders interessant. Im Fall einer erfolgreichen Attacke bieten sie einen besonders großen Hebel für Erpressung und verfügen über große Mengen an sensiblen Daten, die sich gewinnbringend vermarkten lassen.

Gelingt es, eine Schadsoftware in einer öffentlichen Verwaltung, in Krankenhäusern oder bei Stadtwerken zu platzieren, kann dies die Arbeit dieser Organisation umfassend stören oder auch ganz zum Erliegen bringen. Werden die Daten und Systeme zur Erpressung verschlüsselt, müssen umfangreiche Recovery-Maßnahmen durchgeführt werden, und es droht sogar der Verlust von wichtigen Daten. Im schlimmsten Fall fallen solche Einrichtungen für Wochen aus. Dies führt nicht nur zu erheblichen Folgeschäden, sondern kann auch Menschenleben gefährden.

Spam, Malware- und Phishingattacken gehören nach wie vor zu den erfolgreichsten Angriffsformen – auch weil sie sich massenhaft mit großen Reichweiten automatisiert durchführen lassen. Aber auch hochgradig spezialisierte Kampagnen zur Erschleichung von Identitäten mit Social Engineering nutzen E-Mails als Kommunikationsmedium.

Bild: khunkorn - stockadobe.com

Komplettpaket für E-Mail-Sicherheit

Zuverlässiger Schutz vor Spam und Malware, sichere E-Mail-Verschlüsselung, einfacher Versand großer Dateien und mühelose Verwaltung von E-Mail-Disclaimern: Aus vier Modulen kann ein individuelles Paket für E-Mail-Sicherheit zusammengestellt werden.

Sechsfacher Mail Security Champion

NoSpamProxy holte 2023 zum sechsten Mal in Folge den Champion-Titel in der unabhängigen Nutzerbefragung für E-Mail-Security. Die Lösung überzeugt besonders in den Kategorien Leistungsfähigkeit, Funktionsumfang und Benutzerfreundlichkeit.

E-Mail-Security made in Germany

NoSpamProxy trägt das Gütesiegel IT-Security made in Germany und steht seit mehr als 15 Jahren für Zuverlässigkeit und Kompetenz. Es erfüllt alle gesetzlichen Anforderungen und ist vollständig EU-DS-GVO-konform.

Immer mehr öffentliche Einrichtungen wie Kommunen, Landes- und Bundesbehörden, kommunale Versorger, Universitäten oder Krankenhäuser nutzen deshalb die E-Mail-Sicherheits-Suite NoSpamProxy in lokaler Installation oder als Cloud Service.

Mit NoSpamProxy Suite erhalten öffentliche Einrichtungen alle Features für zuverlässigen Schutz vor Malware, Ransomware und Spam mit dem Modul Encryption. Das Modul NoSpamProxy Encryption bietet eine einfache und praxisnahe E-Mail-Verschlüsselung für die datenschutzkonforme Kommunikation per E-Mail – auch mit Empfängern außerhalb der Verwaltungsnetze. Durch NoSpamProxy Large Files und Disclaimer funktioniert das Versenden großer Dateien ohne Probleme, und die Verwaltung von E-Mail-Disclaimern wird mühelos.

> *„NoSpamProxy ist für die hohen Ansprüche im öffentlichen Dienst gerade wegen der hohen Flexibilität ideal. Mit NoSpamProxy bieten wir eine optimale E-Mail-Security, die sich mithilfe der vier Module perfekt an Ihre Bedürfnisse anpassen lässt. Eine Lösung auf höchstem Niveau, mit exzellentem Support und maximaler Benutzerfreundlichkeit – und natürlich made in Germany."*

MATTHIAS WERNER,
Strategic Account Manager NoSpamProxy

Das langjährig bewährte Produkt von Net at Work aus Paderborn beweist seine hohe Wirksamkeit regelmäßig in entsprechenden Tests durch Expertenteams. Es erfüllt die Empfehlungen des BSI sowie alle gesetzlichen Voraussetzungen wie die der EU-DS-GVO. Seit Jahren schneidet NoSpamProxy in unabhängigen Nutzerbefragungen als Champion mit bester Performance und höchster Benutzerfreundlichkeit ab. Sowohl das Produkt – ausgezeichnet mit dem Gütesiegel „IT-Security made in Germany" – als auch der hervorragende Support kommen vollständig aus Deutschland.

Die vier Module sind sowohl in der Cloud als auch als On-Premises-Lösung verfügbar. Zahlreiche öffentliche IT-Dienstleister bieten NoSpamProxy speziell für öffentliche Einrichtungen als Managed Service aus BSI-zertifizierten Rechenzentren an. ■

Vorteile im Überblick

- ✓ Verlässliche Abwehr von Cyberangriffen
- ✓ Sicheres Versenden von sensiblen Daten
- ✓ Preisgekrönter Support in Deutsch und Englisch
- ✓ Erfüllung aller gesetzlichen Anforderungen und der DS-GVO
- ✓ Modulare und flexible Lösung
- ✓ Schadcodefreie E-Mail-Anhänge
- ✓ Keine schadhaften Links in E-Mails
- ✓ Keine E-Mails von falschen Absendern

Mehr dazu hier

DIGITALE KONFERENZ ZUR E-MAIL-SICHERHEIT FÜR ÖFFENTLICHE EINRICHTUNGEN, KOMMUNEN UND VERWALTUNGEN

Diese speziell für öffentliche Einrichtungen, Kommunen und Verwaltungen konzipierte Veranstaltung widmet sich dem wichtigen Thema der E-Mail-Sicherheit als Managed Service. Erfahren Sie mehr über Risiken, Lösungen und gesetzliche Anforderungen.

Gemeinsam mit Kunden und Partnern bieten wir eine Reihe von informativen Vorträgen, in denen die Risiken im Zusammenhang mit E-Mails als potenzielles Einfallstor beleuchtet werden. Experten aus der Branche werden darüber hinaus Lösungen präsentieren, die einen optimalen Schutz von öffentlichen Einrichtungen gewährleisten und dabei die gesetzlichen Anforderungen im Blick behalten.

Themenübersicht

- **Identifizierung und Analyse von Sicherheitsrisiken in E-Mails**
- **Best Practices für den Schutz vor E-Mail-basierten Angriffen**
- **Managed Services zur Sicherstellung der E-Mail-Sicherheit**
- **Rechtliche und gesetzliche Anforderungen im Umgang mit E-Mails in öffentlichen Einrichtungen**
- **Effektive Maßnahmen zur Prävention und Abwehr von E-Mail-Bedrohungen**

Nutzen Sie diese einzigartige Gelegenheit, um sich mit führenden Experten auszutauschen und wertvolles Wissen über die Sicherheit von E-Mails als Managed Service aufzubauen. Die Konferenz bietet außerdem eine ideale Plattform, um Kontakte zu knüpfen und sich mit anderen Fachleuten aus Ihrem Bereich zu vernetzen.

Reservieren Sie sich den Termin schon jetzt in Ihrem Kalender.

Wir freuen uns darauf, Sie bei der digitalen Konferenz begrüßen zu dürfen!

Reservieren Sie Ihren Platz!

19.09.2023, 09.00 bis 12.00 Uhr.

www.nospamproxy.de/de/digitalekonferenz/

noSpam proxy®

sosafe

(ISC)² Sammeln Sie CPE-Credits!

HUMAN RISK REVIEW 2023

Neue Brancheneinblicke von führenden Security-Expertinnen und -Experten

- 9 ausführliche **Interviews** mit Security-Führungskräften
- **Umfrage** unter Expertinnen und Experten zum Stand von **Cyber Security in Europa**
- Detaillierte **Social-Engineering-Analysen** zu den erfolgreichsten Taktiken der Cyberkriminellen