Nr. 65/2022

tele-news

TIPPS UND TRENDS FÜR IHRE TELEKOMMUNIKATION

Hösel
Fernmelde- & Computerservice

Mario Hösel
Geschäftsführung
Fernmelde- & Computerservice
Hösel

Liebe Leserin, lieber Leser,

Firewalls, Antivirenschutz, Netzwerkkontrolle – gegen Cyberangriffe von außen haben die meisten Unternehmen Maßnahmen ergriffen. Doch der menschliche Faktor, das macht eine aktuelle Studie deutlich, wird als Risikopotenzial gravierend unterschätzt.

Mit Security Awareness-Schulungen kann das Sicherheitsbewusstsein im Unternehmen erheblich gesteigert werden. Wir stellen Ihnen hier die Lösung von Kaspersky Lab vor. Einsichten über mögliche Risiken in Ihrer Microsoft 365-Umgebung und deren proaktive Beseitigung ermöglicht Ihnen Policies & Insights von AvePoint.

223 Mrd. Euro Schäden durch Cyberangriffe im vergangenen Jahr: ***Sichern Sie Ihr Unternehmen jetzt!***

STUDIE CYBER-SECURITY 2022

Gefahr von innen

Die beste IT-Security bringt nichts, wenn der Faktor Mensch das größte Sicherheitsrisiko darstellt. Die aktuelle Cyber-Security-Studie 2022 von CIO, CSO und Computerwoche stellt deshalb diesen Aspekt in den Vordergrund ihrer Untersuchung und empfiehlt Unternehmen die Durchführung von verpflichtenden Security-Awareness-Programmen.

Interne Vorfälle durch eigene Beschäftigte haben laut Studie für etwa 50 Prozent der befragten Unternehmen das Potenzial für kritische oder katastrophale Folgen. Allerdings glauben viele, dass diese kritischen Vorfälle bei ihnen selbst gar nicht eintreten. Gerade das Risiko durch „Innentäter“ wird also zum einen gefürchtet, dann aber im eigenen Unternehmen als nicht so wahrscheinlich eingestuft – obwohl mehr als die Hälfte der Unternehmen genau solche Insidervorfälle bereits erlitten hat.

Täter ohne böse Absicht

Unter „Innentäter“ versteht die Studie keine kriminellen Datenräuber, die sich in ein Unternehmen eingeschleust oder gehackt haben. Vielmehr sind es Menschen aus den Reihen der eigenen Beschäftigten, die ohne jede böse Absicht zu Tätern werden, indem sie Unternehmensdaten, Account-Informationen, Passwörter oder auch Geschäftsgeheimnisse fahrlässig oder unbewusst an Unbefugte weitergeben, ohne sich der möglichen Konsequenzen bewusst zu sein.

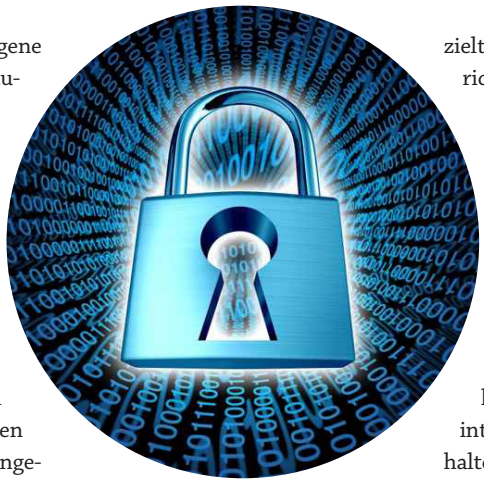


Illustration: freshidea/fotolia

Mittels Social Engineering gelangen Kriminelle trotz aller Security-Maßnahmen immer noch viel zu einfach und schnell an ihr Ziel, indem sie menschliche Schwachstellen ausnutzen. Hier spielt vor allem das Phishing per E-Mail eine Rolle: Welcher Mitarbeiter kontrolliert schon, ob die Mail, deren unverdächtigen Anhang er öffnet, wirklich vom Chef kommt? Oder die Anforderung der angeblichen IT-Abteilung, auf einen Link zu klicken, damit der neue Account bestätigt wird?

Cyberkriminelle können solche Phishing-E-Mails täuschend echt aussehen lassen und sie gezielt auf einzelne Personen ausrichten. Durch die zunehmend zeitlich und räumlich flexible Arbeit (Homeoffice, Hybrid Work) werden die Risiken für Security-Verletzungen und daraus resultierenden Angriffen noch erhöht. Als zentrale Sicherheitsstrategie für Hybrid Work gilt Zero Trust. Der Kerngedanke: Nicht mehr zu glauben, interne Vorgänge oder das Verhalten von Mitarbeitern seien weniger gefahrenträchtig als externe. Für ein Security-Konzept bedeutet dies, Zeit und Ressourcen nicht nur in die technische IT-Sicherheit zu investieren, sondern auch in den menschlichen Faktor.

Sicherheitsbewusstsein aufbauen

Das Resümee der aktuellen Studie: „Jedes Unternehmen kann von Cyber-Attacken getroffen werden und sei es Security-technisch noch so ‚hochgerüstet‘. Was die menschliche Fehlerkomponente betrifft, helfen nur umfassende, regelmäßige und verpflichtende Security-Awareness-Programme – immer und immer wieder wieder, egal wie nervtötend sie sein mögen.“ ■

KASPERSKY SECURITY AWARENESS PLATTFORM

IT-Sicherheit durch informierte Mitarbeiter

Kann ich unbesorgt auf einen Bestätigungslink klicken, der mir per E-Mail zugesandt wird? Sind meine Passwörter sicher? Woran erkenne ich eine Phishing-Website? Dies sind Beispielsituationen in einem spielerischen Test bei dem Mitarbeiter in nur 15 Minuten zwölf alltägliche, für die Cybersicherheit relevante Situationen durchlaufen. Der spielerische Ansatz motiviert die Mitarbeiter und zeigt gleichzeitig, wo nach Analyse der dargestellten Situationen noch Wissenslücken bestehen.

Foto, Grafik: Kaspersky

Der überwiegende Teil aller Angriffe auf die IT sind auf menschliche Fehler zurückzuführen. Fehler, die ein Unternehmen Millionen kosten können. Mit der Awareness Plattform von Kaspersky trainieren und sensibilisieren Sie Ihre Mitarbeiter und beugen so Cyberangriffen vor.

Im vergangenen Jahr summierten sich die Verluste der deutschen Wirtschaft durch Cyber-Kriminalität auf den Rekordwert von 223 Milliarden Euro. 88 Prozent der Firmen gaben laut Angaben des Branchenverbands Bitkom an, Opfer von Angriffen gewesen zu sein. Insbesondere beim Mittelstand hat es einen starken Zuwachs gegeben.

Dass viele Unternehmen in der Pandemie verstärkt Mitarbeitende im Homeoffice eingesetzt haben, hat zu der enormen Steigerung der Schäden beigetragen. Zusätzlich zur Security-Architektur im Unternehmen müssen auch die Systeme im Homeoffice und ihre Verbindungen zur Zentrale geschützt werden. Für Cyber-Kriminelle ergeben sich daraus deutlich mehr Einfallstore als vor der Corona-Pandemie.

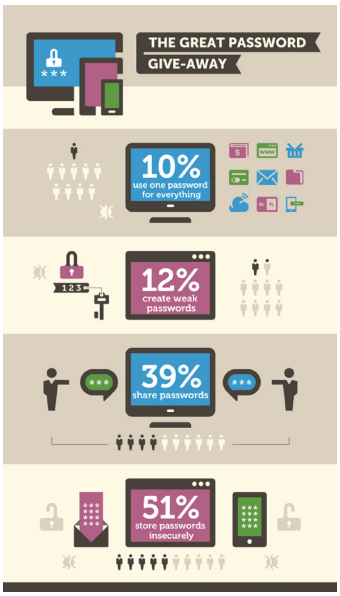
Schlecht informierte Mitarbeiter sind ein Sicherheitsrisiko

Bei den Cyberangriffen wurden vor allem Attacken auf Passwörter, Phishing und die Infizierung mit Schadsoftware bzw. Malware für die Unternehmen teuer. Einen deutlichen Anstieg gab es beim sogenannten Social Engineering. Fast jedes zweite Unternehmen berichtet von entsprechenden Versuchen, über die Belegschaft Sicherheitslücken aufzutun und diese zu Attacken zu nutzen. Bitkom-Präsident Berg: „Eine regelmäßige Schulung von Mitarbeiterinnen und Mitarbeitern zu Sicherheitsfragen, damit sie sich auch bei Social-Engineering-Versuchen richtig verhalten, sollte in jedem Unternehmen selbstverständlich sein."

Je mehr Mitarbeiter wissen, wie man sich vor den Machenschaften krimineller Hacker schützt, desto sicherer ist das Unternehmen. Mit seiner Strategie der Security Awareness zeigt Kaspersky einen effektiven Weg zum Aufbau einer umfassenden IT-Sicherheit.

Durchdachtes Schulungsprogramm für Security Awareness

Die Automated Security Awareness Plattform von Kaspersky Lab ist ein Online-Tool zum Aufbau umfassender und praktischer Kenntnisse zur Cybersicherheit. Sie unterstützt damit Unternehmen jeder Größenordnung auf dem Weg hin zu einer sicheren IT-Umgebung. Spezifische Ressourcen und Vorbereitungen sind für die Implementierung und Verwaltung der Plattform nicht erforderlich.



Eine Reihe von interaktiven Programmen bildet bei Kaspersky Security Awareness ein umfassendes Schulungsportfolio, das sich an alle Ebenen des Unternehmens richtet. Die Grundlage: Mithilfe spielerischen Lernens, z. B. in Online-Planspielen, können Situationen und deren Konsequenzen „durchlebt" und daraus Handlungsstrategien für die IT-Sicherheit entwickelt werden.

Security ist Chefsache

Die größte Herausforderung für IT-Sicherheitsverantwortliche in Unternehmen besteht laut Kaspersky allerdings darin, Führungskräfte für die Sache der IT-Security zu motivieren. Erst wenn der Belegschaft eine Sicherheitskultur vorgelebt wird, kann sich ein abteilungsübergreifendes Sicherheitsbewusstsein etablieren.

Speziell für IT-Sicherheitsteams und das Management bietet Kaspersky deshalb ein Übungsszenario, bei dem das Unternehmen in eine simulierte Geschäftsumgebung versetzt und einer Reihe unerwarteter Cyberbedrohungen ausgesetzt wird. Auf diese Weise lassen sich die typischen Fehler beim Aufbau der IT-Sicherheit ermitteln und es kann eine effektive und effiziente Verteidigungsstrategie entwickelt werden.

Wenn die Qualität stimmt, sind Awareness-Trainings erwiesenermaßen die effektivste Methode, um das Risiko von Angriffen auf das Unternehmensnetzwerk zu minimieren. Eine wichtige Aufgabe, die mit Kaspersky Security Awareness erfolgreich bewältigt werden kann. ■

Kaspersky Security Awareness bietet mit seinen interaktiven Schulungsplattformen für alle Unternehmensebenen effektive, nachhaltige und messbare Ergebnisse bei der Qualifizierung und Ertüchtigung der IT-Sicherheitsarchitektur im Unternehmen. Durch „Edutainment" werden die Schulungsteilnehmer spielerisch einbezogen und motiviert, durch Abrufen des Gelernten in der Berufspraxis werden die neu erworbenen Kompetenzen verinnerlicht und geraten nicht wieder in Vergessenheit.

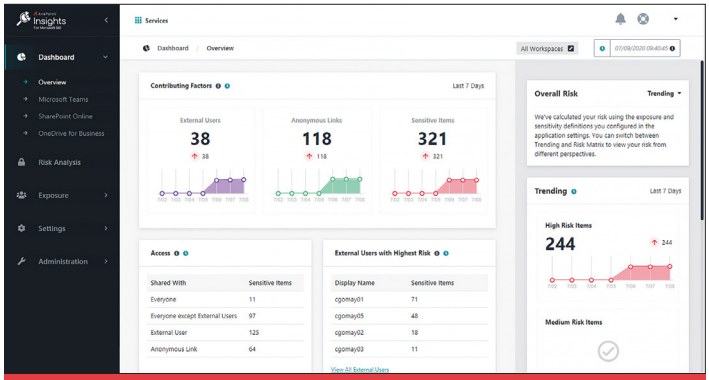
Risikomanagement für Microsoft 365

Fotos/Illustrationen: Avepoint

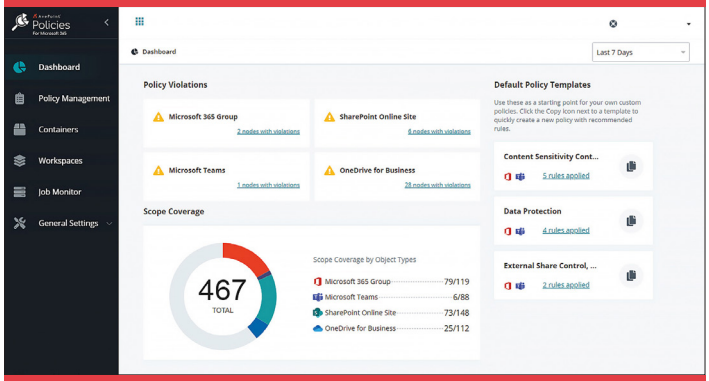
Microsoft 365 bildet mit Komponenten wie Teams, OneDrive, SharePoint etc. ein mächtiges Instrument, mit dem die Effektivität und Effizienz von Kollaborationsstrukturen im Unternehmen erheblich gesteigert werden kann. Die vielfältigen Möglichkeiten können bei unorganisierter Zusammenarbeit von Nutzern jedoch einen Wildwuchs bei der Datenerstellung und Übersichtlichkeit hervorrufen. Mit Avepoint Policies & Insights behalten Sie die Kontrolle.

Die Bildung von (temporären) Teams ist für die strukturierte Arbeit im Unternehmen eine sinnvolle Maßnahme. Mit Microsoft 365 ist die digitale Basis für solche Teams schnell etabliert. Weil dies so einfach zu machen ist, wird diese Möglichkeit auch gern genutzt. Manchmal allzu gern. Denn wenn die Übersicht verloren geht, welche Teams woran arbeiten, welche Mitarbeiter in welchen Teams sind und ob diese Teams noch alle aktiv sind, stellt dies ein potenzielles Sicherheitsrisiko dar.

Ein weiteres Beispiel: Die manuelle Erfassung von Nutzerberechtigungen oder von geteilten Links in Microsoft 365 ist zeitintensiv und komplex. Hier den Überblick zu behalten, kann für Unternehmen ohne damit befasste IT-Mitarbeiter eine schwer zu bewältigende Aufgabe sein. Außerdem können sogar gründliche Analysen innerhalb von kurzer Zeit veraltet sein. Dies kann sich zu einer ernsthaften Sicherheitslücke auswachsen.



Was spielt sich ab in Microsoft 365? AvePoint Policies and Insights gibt Einblicke.



Mit detaillierten Sicherheitsberichten werden mögliche Risiken stets aktuell abgebildet.

Risiken in der Microsoft 365-Umgebung erfassen

Die Lösung heißt AvePoint Policies & Insights (PI). PI wurde entwickelt, um die mit sensiblen Dokumenten verbundenen Risiken sowie den Zugriff darauf zu analysieren und Richtlinienverstöße in Microsoft 365 proaktiv festzustellen und zu beheben. Mithilfe von Sicherheits-Dashboards kann die Veränderung des Risikopotenzials (anonyme Links, externer Zugriff durch Nutzer) zudem laufend hervorgehoben und nachverfolgt werden. Aktualisierungen in Quasi-Echtzeit, die die am häufigsten geteilten sensiblen Daten priorisieren, ermöglichen es, Eigentümer- und Freigabebeschränkungen einzuführen, die eine sichere Zusammenarbeit unterstützen.

AvePoint Policies and Insights erleichtert die Überwachung von Microsoft 365-Berechtigungen mit detaillierten Sicherheitsberichten. Dazu werden Microsofts eigene Sicherheits-, Aktivitäts- und Compliance-Feeds verwendet, um Sensitivitäts- und Aktivitätsdaten über Teams, Gruppen, SharePoint und OneDrive hinweg zu erfassen. Anschließend werden kritische Probleme basierend auf der individuellen Risikodefinition des Unternehmens oder der Organisation priorisiert, sodass das IT-Team gezielt Maßnahmen ergreifen kann. Sicherheits-Dashboards helfen dabei, das verringerte Risiko und den Fortschritt im Laufe der Zeit für anonyme Links, externen Nutzerzugang und Schattennutzer aufzuzeigen.

Kontinuierliche Überwachung

Pi überwacht den Zustand von Microsoft 365, sodass leicht festgesellt werden kann, wer Zugang zu sensiblen Daten hat, ob diese Personen darauf zugegriffen haben und ob externe Nutzer eine Gefahr darstellen. Dabei kann definiert werden, welche Vorgänge für das Unternehmen als Risiko zu bewerten sind und welche entsprechenden Richtlinien oder Microsoft 365-Berechtigungskontrollen angewandt werden sollen. Mit PI lassen sich allgemeine Regeln für Zugriff, Einstellungen und andere Konfigurationen für Teams, Gruppen, Sites und OneDrive leicht erstellen und automatisieren. Wenn PI eine Konfigurationsänderung erkennt, wird darüber automatisch benachrichtigt und die Änderungen werden gegebenenfalls rückgängig gemacht.

Grundlegende Berechtigungsberichte können mit Microsoft Sensitive Information Types und Microsoft Activity Feed-Daten verknüpft werden. Durch die Priorisierung von sensiblen Inhalten, externen Nutzern, mittlerweile nicht mehr berechtigten Nutzern und anonymen Links kann das IT-Team dort Maßnahmen ergreifen, wo sie die größte Wirkung haben.

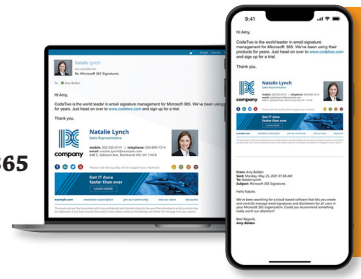
Ergebnisse kontrollieren

AvePoint Policies and Insights zeigt auf, welche Auswirkungen Adhoc- und automatisierte Sicherheitskorrekturen mit sich bringen. Dashboards belegen den Fortschritt, sodass nachvollziehbar ist, wie effektiv die Probleme behandelt werden.

Fazit: Mit AvePoint Policies and Insights lassen sich potenzielle Risiken im Unternehmen mit wenigen Klicks ermitteln. Änderungen in der Microsoft 365-Umgebung werden zusammengefasst, risikoreiche Maßnahmen, die weitere Schritte erfordern, werden identifiziert und nach Priorität geordnet. Der Einsatz von AvePoint Policies and Insights entlastet das IT-Team, macht Ressourcen frei, verhindert proaktiv Sicherheitslücken und spart so nachhaltig Kosten. ■

Visitenkarten des Unternehmens

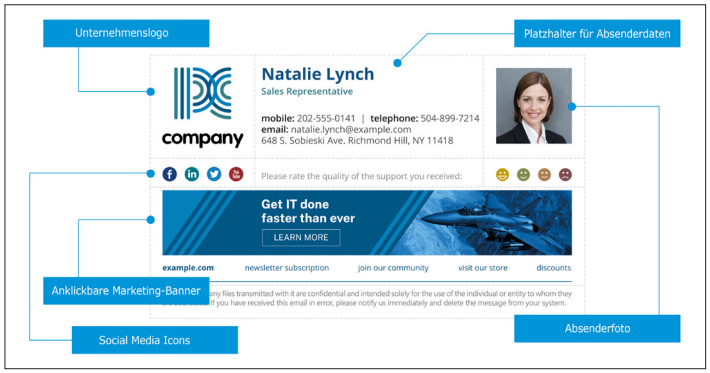
Wenn im Unternehmen unterschiedlichste E-Mail-Signaturen und Disclaimer im Umlauf sind, kann das schnell unübersichtlich werden. CodeTwo für Microsoft 365 bietet dafür die perfekte Lösung.



CodeTwo E-Mail-Signaturen informieren nicht nur den Empfänger über die Kontaktdaten des Absenders. Mit integrierten Text- und Bildelementen ermöglichen sie darüber hinaus die Übermittlung von Informationen, die aus der Marketingperspektive oder für die Kundenkommunikation wichtig sind. Dies bedeutet, dass sie als leistungsstarkes und kostengünstiges Medium für die Marketing- und Kundenkommunikation genutzt werden können.

CodeTwo E-Mail-Signaturen für Office 365 arbeitet mit allen E-Mail-Apps und -Geräten sowohl für Windows als auch für Mac, für Desktops, Handys und Tablets.

CodeTwo E-Mail-Signaturen für Office 365/Microsoft 365 ist ein Cloud-Dienst, der das Erstellen und organisationsweite Verwalten von E-Mail-Signaturen, Disclaimern, automatischen Antworten und Marketingkampagnen unternehmensweit und abteilungsübergreifend ermöglicht.



CodeTwo E-Mail-Signaturen für Office 365 bindet Logos, Social Media Buttons, Marketingbanner, Office 365/Microsoft 365-Benutzerfotos und vieles mehr automatisch in die Signatur ein.

Im „Quick Customization"-Fenster können E-Mail-Vorlagen sehr einfach mit einem Mausklick zur Aktivierung oder Deaktivierung eines Signaturbereichs angepasst werden.

Flexibel konfigurierbar

CodeTwo E-Mail-Signaturen bieten zahlreiche Personalisierungsmöglichkeiten. Dabei kann u.a. festgelegt werden, wann die Vorlagen zu E-Mails hinzugefügt werden sollen und welche Benutzer auf eine bestimmte Signaturvorlage in Outlook zugreifen dürfen. Die Signaturregeln erlauben praktisch jede Art von Automatisierung. So können Signaturen nur bestimmten Absendern hinzugefügt werden oder auf der Nationalität der Empfänger, den Schlüsselwörtern im E-Mail-Inhalt und anderen Variablen basieren. Weiterhin können die Signaturvorlagen dynamische Felder erhalten, die beim Versand automatisch durch Attribute eines Benutzers ersetzt werden.

Vorteile für Ihr Unternehmen

Mit dem CodeTwo Signaturmanager für Microsoft 365 können Sie:

- E-Mail-Signaturen und -Disclaimer zentral für das Unternehmen verwalten.
- Automatisch die Kontaktangaben des Absenders hinzufügen.
- Marketingbanner, Benutzerfotos und Social-Media-Buttons in E-Mail-Signaturen einbetten: Sie müssen sie nicht mehr verlinken. So werden diese Elemente immer angezeigt, ohne dass die Empfänger sie herunterladen müssen.
- Signaturen direkt unter Antworten oder Weiterleitungen einfügen.
- Signaturen direkt in Outlook und OWA hinzufügen oder automatisch in der Cloud, nachdem die E-Mail gesendet wurde. Dies gilt für alle E-Mail-Clients und Geräte (einschl. Mobilgeräte und Mac).
- Professionelle E-Mail-Signaturen mit einem leistungsstarken und leicht zu bedienenden HTML-Editor für eigene Signaturvorlagen oder integrierte Vorlagen von CodeTwo nutzen und nach Bedarf anpassen.
- Regeln erstellen, die bestimmen, wann E-Mails Signaturen erhalten ...
- ... und vieles mehr.

Immer konform mit dem Unternehmens-Branding

Im serverseitigen Modus fügt CodeTwo E-Mail-Signaturen für Office 365 ausgehenden Nachrichten Signaturen und Haftungsausschlüsse in der Cloud hinzu. Dies geschieht auf der Basis von vorher Gruppen entsprechen. Und das Beste daran ist, dass diese Signaturen immer konform mit der CI und dem Corporate Design des Unternehmens sind.

CodeTwo E-Mail-Signaturen wurde von Microsoft auf Sicherheit, Compliance und Datenverarbeitungspraktiken überprüft und als bisher einziger Anbieter von Signatur-Software zertifiziert. ■

Impressum

Redaktion: Karl-Heinz Zonbergs

Herausgeber: Mario Hösel (V.i.S.d.P.)
Fernmelde- & Computerservice Hösel
Blumenstraße 1
09526 Olbernhau
Telefon(0 37 360) 69 08-0
Telefax(0 37 360) 69 08-50
Internet: www.fernmeldeservice.de
E-Mail: info@fernmeldeservice.de

Layout: Ulrike Hartdegen
E-Mail: layout@ulrikehartdegen.de

Anschrift der Redaktion:
BestWord
Kappenstraße 70
45473 Mülheim an der Ruhr
Telefon (02 08) 76 24 99
Telefax (02 08) 76 23 92
E-Mail: info@bestword.de