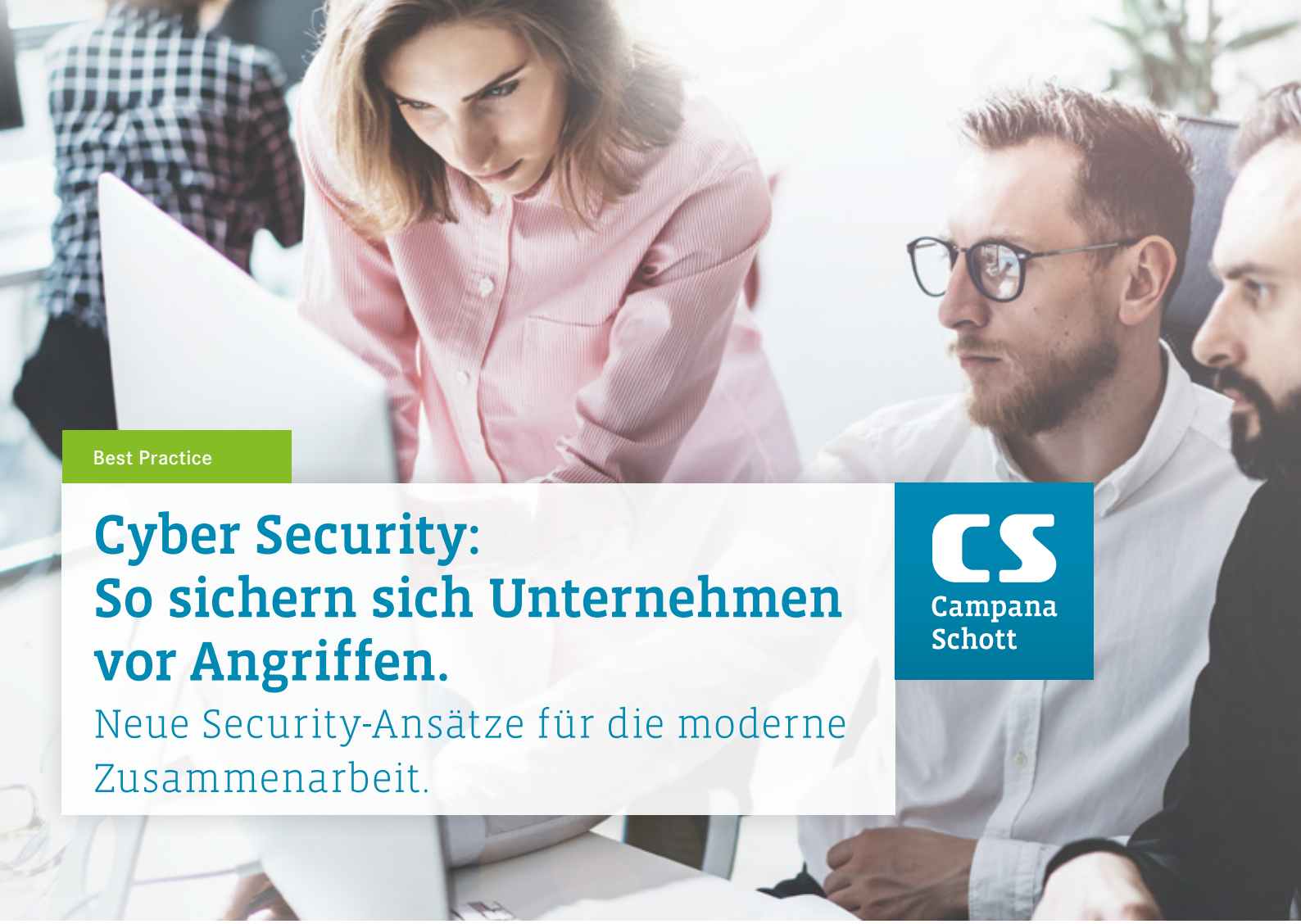

Best Practice

Cyber Security: So sichern sich Unternehmen vor Angriffen.

Neue Security-Ansätze für die moderne Zusammenarbeit.

Campana Schott

Cyberkriminelle greifen heutzutage Unternehmen unabhängig von deren Größe und Branche an. Gleichzeitig wandelt sich das Arbeits- und damit auch IT-Umfeld massiv und es entstehen intelligentere Angriffsmethoden, vor denen sich Unternehmen schützen müssen. Wir zeigen, welche Methoden greifen, um Unternehmen zu schützen und die IT Security Awareness zu erhöhen.

Unternehmen investieren zunehmend in moderne Cloud-basierte Formen der Zusammenarbeit im Rahmen des Digital Workplace. Dies zeigt etwa die Deutsche Social Collaboration Studie 2019. Demnach stieg der Reifegrad deutscher Firmen auf einer Skala von 1 bis 7 im Vergleich zum Vorjahr von 3,96 auf 4,05. Doch knapp zwei Drittel der Befragten sind nicht damit zufrieden, wie Social-Collaboration-Tools bisher in ihrem Unternehmen eingeführtwurden. Dies liegt hauptsächlich an mangelnder Berücksichtigungkonkreter Bedürfnisse einzelner Mitarbeiter und zu wenig Zeit, sich mit den Tools auseinanderzusetzen.

Gerade Millennials fordern heute eine einfache Art der Zusammenarbeit und Nutzung der Anwendungen zu jeder Zeit, an jedem Ort und auf unterschiedlichen Geräten. Aufgrund dieser Mobilität und Flexibilität des digitalen Arbeitsplatzes reichen klassische IT-Sicherheitsansätze mit Fokus auf den Netzwerk-Perimeter nicht mehr aus. Denn moderne Zusammenarbeit benötigt auch eine dazu passende moderne Security-Architektur.

Genau hier sehen Cybersecurity-Experten derzeit die größten Risiken. Dazu gehören vor allem die Nutzung von Cloud-Infrastrukturen und mobilen Geräten, die Datenhaltung in Public-Cloud-Lösungen sowie das oft fehlende Risikobewusstsein von Anwendern. Laut dem Cisco Annual Cybersecurity Report 2018 nutzen Cyberkriminelle zunehmend Cloud-Services und IoT-Botnetze für ihre Angriffe. Zu den wichtigsten Security-Trends 2019 gehören gemäß DXC Technology ein zunehmender Zugriff von Kriminellen auf Endpoints, um gezieltere Ransomware-Angriffe durchzuführen, sowie ein Zero-Trust-Modell, bei dem Unternehmen prinzipiell niemandem mehr trauen – ob innerhalb oder außerhalb des Perimeters.

Vor Gefahren schützen

Doch wie kann ein Unternehmen den Digital Workplace am besten schützen? Dazu dienen insbesondere drei Komponenten:

1. **Sicherung der Identität im Cyberspace**
2. **Konsequenter Schutz der Unternehmensdaten**
3. **Nachhaltige IT Security Awareness Maßnahmen**

Um die Identität abzusichern, reichen Malware-Filter auf Signatur-Basis nicht mehr aus. Auch unbekannte Angriffe müssen etwa mit Hilfe von Machine Learning über Anomalien erkannt und rechtzeitig abgewehrt werden. Zudem sollte ein Zero-Trust-Modell immer kombiniert sein mit adäquaten Passwort-Richtlinien und bei Bedarf Multi-Faktor-Authentifizierung, ohne jedoch die Produktivität dadurch einzuschränken.

Der Schutz der Unternehmensdaten ist gerade auf mobilen Geräten elementar. Daher sollte ein modernes Mobile Device Management zum Einsatz kommen, das idealerweise mit den Maßnahmen zum Schutz der Identitäten verknüpft wird. Zur Ergänzung bieten sich Werkzeuge für die Dokumentenklassifizierung und Erkennung sensibler Informationen an, die als Basis für Maßnahmen im Compliance Umfeld, speziell im Rahmen von Data Loss Prevention oder zur Einhaltung der DSGVO dienen.

IT Security Awareness

Die IT Security Awareness umfasst vor allem zwei Aspekte. Da selbst ein moderner Malware-Schutz niemals sämtliche Phishing-Mails ausfiltern kann, müssen Mitarbeiter verstehen, wie Phishing funktioniert und wie sie solche Angriffe erkennen und verhindern können. Zusätzlich sollten sie nachvollziehen, warum ein komplexes Kennwort wichtig ist und welche Risiken bestehen, wenn es mehrfach verwendet wird.

Diese Awareness lässt sich einerseits durch klassische Ansätze wie IT-Security-Trainings vor Ort oder Web-basiert erhöhen. Andererseits können praktische Tests wie simulierte Phishing-Angriffe den Mitarbeitern die Augen öffnen. Hier werden Anwender, sobald sie auf den Inhalt oder Anhang der Mail klicken, über die Risiken und mögliche Maßnahmen zur Erkennung solcher Angriffe direkt informiert. Idealerweise erhält ein Unternehmen bei einer solchen Kampagne auch eine Aussage darüber, wie hoch die Awareness seiner Mitarbeiter gegenüber Phishing-Angriffen ist.

Schritt 1: Assessment

Welche Schritte sollten Unternehmen durchführen, um diese drei Komponenten zu verbessern? Am Anfang steht in der Regel ein Assessment, um den aktuellen Status in Bezug auf Security zu ermitteln. Dabei ist nicht nur auf die Verwendung einzelner Sicherheitsprodukte oder -funktionen zu achten, sondern auch darauf, ob zuverlässige Prozesse etabliert sind, die ständig ausgeführt und regelmäßig aktualisiert werden. So nützt zum Beispiel das beste Security-Tool nichts, wenn kein Update durchgeführt wird. Diese Prozesse können aber auch zum Review von Security-relevanten Events dienen oder für sicheren Zugriffsschutz auf Basis von Geräten, Nutzeridentitäten oder Anwendungen sorgen.

Im Microsoft-Cloud-Umfeld lässt sich hierzu etwa der Microsoft 365 Secure Score als Ansatzpunkt verwenden. Er zeigt auf, welche Security-Komponenten im Einsatz sind, und analysiert die Sicherheit einer Organisation auf Basis ihrer regulären Aktivitäten sowie Sicherheitseinstellungen in Office 365 und bewertet diese. Doch unabhängig von Tools oder Methodik erhält das Unternehmen durch ein umfassendes Assessment einen guten Überblick über den Status Quo. Dieser dient als Basis für eine mögliche längerfristige Security-Strategie, kann aber auch Input für schnell umzusetzende Quick Wins geben.

Schritt 2: Roadmap und Strategie

Dieser Schritt sollte alle geplanten Maßnahmen umfassen, um gegenseitige Abhängigkeiten festzustellen. Dabei ist nicht nur die Einführung zu planen, sondern auch der spätere Betrieb. Zudem sollte er auf die Fähigkeiten und Ressourcen des eigenen IT-Security-Bereichs abgestimmt werden. Wenn etwa über Lizenzbündelung bei Microsoft eine Vielzahl an Security-Produkten verfügbar ist, muss das Team die genutzten Tools auch betreiben können.

Die Priorisierung der Roadmap und Strategie sollte auf einer Risikoeinschätzung basieren. Relevante Faktoren sind hier eine Selbsteinschätzung der Angriffsrisiken, aktuelle Angriffsszenarien sowie Aufwand und Komplexität der Umsetzung und des Betriebs. Zudem sind die Maßnahmen regelmäßig zu prüfen und zu aktualisieren, da sich sowohl Security-Funktionen als auch Risiken und Bedrohungen ständig weiterentwickeln.

Schritt 3: Phishing-Kampagne

Eine Phishing-Kampagne sollte sowohl einen Einblick in die Phishing Awareness bieten als auch diese steigern. Dazu werden Phishing-Testmails an die Mitarbeiter verschickt. Wer darauf klickt, erhält eine Information, dass er Opfer von Phishing geworden ist. Anschließend gibt es Hinweise, wie er künftig solche Mails erkennen und sich davor schützen kann.

Üblicherweise steigt die Komplexität solcher Testmails. Während die erste Mail leicht als Phishing-Versuch zu erkennen ist, wird dies sukzessive immer schwieriger. Am Ende erhält das Unternehmen eine anonymisierte Auswertung, bei Bedarf pro Abteilung. Allerdings sollten solche Kampagnen regelmäßig wiederholt werden, um die Awareness kontinuierlich zu verbessern.

Fazit

Auch in der heutigen agilen IT-Welt sind zwar nach wie vor klassische Schutzlösungen wie Antivirus und Firewall sowie ein umfassendes, schnelles Patch- und Update-Management weiterhin unerlässlich. Denn unzureichend abgesicherte oder nicht aktualisierte Systeme bilden im Falle eines Angriffs leichte Ziele. Zum Beispiel wären viele der erfolgreichen WannaCry-Angriffe durch regelmäßige Updates einfach zu verhindern gewesen. Doch dies allein genügt heute nicht mehr.

So ist eine hohe IT Security Awareness der Mitarbeiter nötig, damit sie intelligente Angriffe auf Anwendungen und Endpoints erkennen, die technische Systeme übersehen. Externe Experten können dabei helfen, ein objektives Security Assessment durchzuführen. Dabei wird auch eine Roadmap erarbeitet, mit der sich die Sicherheit im Unternehmen erhöhen lässt, ohne die Produktivität zu gefährden.

Aber auch eine gemeinsam entwickelte IT Security Awareness Kampagne mit einer Phishing-Simulation als Kernkomponente zur Erhöhung der Awareness kann wahre Wunder bewirken. Nur mit einer solchen umfassenden Security-Strategie können Unternehmen den Digital Workplace zuverlässig absichern..