RISIKEN DURCH HANDYNUTZUNG IN UNTERNEHMEN MINIMIEREN

Ohne Smartphones ist das Geschäftsleben nicht mehr denkbar. Doch Unternehmen müssen IT-Sicherheit und Datensicherheit gewährleisten, um enorme Folgeschäden zu verhindern. Viele Risiken lassen sich deutlich verringern, wenn Mitarbeitende dafür sensibilisiert werden und klare Nutzungsregeln existieren.

Cyberangriffe verursachen Schäden in Milliardenhöhe

Der finanzielle Schaden durch Cybercrime betrug 2019 allein in Deutschland rund 88 Millionen Euro. Während der durchschnittliche Schaden knapp 22.000 Euro beträgt, wächst diese Summe deutlich mit der Unternehmensgröße an. Durchschnittlich sollen Spitzenunternehmen täglich mehr als 33.000 Euro durch Cyber-Security-Verletzungen verlieren.

Schützen muss sich jeder: 2021 gaben in Deutschland 46 % der befragten Unternehmen an, sie seien in den letzten zwölf Monaten von einem Cyberangriff betroffen gewesen. Oft verläuft ein Angriff jedoch auch unbemerkt. Bis eine Verletzung der IT-Sicherheit auffällt und behoben werden kann, vergehen rund 280 Tage.

Cyberkriminalität ist ein einträgliches Geschäft und die Zahlen steigen. Jeden Tag kommen rund 100.000 bösartige Websites und 10.000 schädliche Dateien hinzu. Bis 2025 rechnen Marktbeobachter mit einem Schaden von rund 10 Billionen Euro jährlich.

Dennoch schützen sich viele Unternehmen nicht ausreichend. So hat nur rund die Hälfte eine Risikobewertung durchgeführt. Besonders pikant: Jeder Mitarbeitende hat im Durchschnitt Zugriff auf rund 11 Millionen Dateien. Besser geschützt sind davon lediglich fünf Prozent. Dadurch kann bereits durch eine kleine Unachtsamkeit eines einzelnen Mitarbeitenden erheblicher Schaden entstehen. Und menschliche Fehler sind häufig: Zu rund 85 % sind sie die Grundlage für einen Cyberangriff.

Vor Cyberangriffen schützen

Einen 100 %-igen Schutz vor Cyberangriffen gibt es nicht. Jedoch existieren Maßnahmen, die es Cyberkriminellen so schwer wie möglich machen. Dafür stellen wir Ihnen wichtige Tipps vor.

Für den Notfall vorzusorgen, bleibt auch bei den striktesten Vorkehrungen sinnvoll. So verhindert eine Backup-Strategie, dass zu viele Daten verloren gehen. Zusammen mit einem Notfallplan sorgt sie dafür, dass die Systeme nach einem Angriff schnell wieder einsatzbereit sind.

Einen Cyberangriff zu erkennen, kann sich zudem als schwierig erweisen, denn nicht jede Malware sperrt gleich das gesamte System. Egal ob ungewöhnliche Übertragungen und Abfragen von Daten, verdächtige Login-Aktivitäten oder andere Folgen: Oftmals benötigt es eine fähige IT-Abteilung, um Angriffe schnell zu identifizieren.

Handynutzung birgt Risiken

Vor allem die Risiken bei der Nutzung von mobilen Endgeräten werden häufig unterschätzt. Gerade kleinere Unternehmen sind sich nicht bewusst, welche Gefahr von der privaten Nutzung der Firmenhandys ausgeht. Doch auch die berufliche Nutzung von eigenen Geräten, wie sie bei BYOD (Bring Your Own Device) üblich ist, birgt diverse Risiken. Denn zum einen stellen nicht ausreichend geschützte Endgeräte ein Sicherheitsrisiko dar. Zum anderen drohen (unbewusst) Verstöße gegen die DSGVO. Dies geschieht bereits dann, wenn Daten auf Servern hochgeladen werden, die sich nicht in der EU befinden. Das ist beispielsweise bei WhatsApp der Fall, einem der am häufigsten genutzten Messenger in Deutschland. Mehr Details zu den Tücken der Mischnutzung erfahren Sie in unserem Beitrag *Firmenhandy: Private Nutzung*.

Die wichtigsten Sicherheitstipps für Unternehmen

1. Mitarbeiter sensibilisieren

Einer der wichtigsten Faktoren ist die Sensibilisierung der Belegschaft für Cyberkriminalität und ihre Folgen. Sie ist die Grundlage dafür, dass der Umgang mit mobilen Endgeräten und auch die Nutzung des Firmennetzwerks sicher ist. Diese Maßnahme ist aufwändig, jedoch unumgänglich. Schließlich sind in bis zu neun von zehn Fällen menschliche Fehler Ursache der Sicherheitslücke. Regelmäßige Schulungen helfen Mitarbeitenden dabei, solche Fehler zu vermeiden und auch zu verstehen, warum das so wichtig ist.

2. Strikte Passwort-Vorgaben

„12345“, „passwort“ oder „hallo“: Viele Menschen nutzen diese Top 3 der unsicheren Passwörter. Das Risiko: Wem die Benutzerkennung bekannt ist, kommt problemlos an zugriffsgeschützte Daten. Um dies zu verhindern, sollten Unternehmen konkrete Anforderungen an geschäftlich genutzte Passwörter stellen. Sinnvoll sind mindestens 7 Zeichen, in denen zudem Varianz herrscht: Groß- und Kleinbuchstaben, Satzzeichen und Zahlen sollten enthalten sein. Besonders sicher sind Passwörter, die nicht im Wörterbuch zu finden sind. Auch eine Zwei-Faktor-Authentifizierung sollten Mitarbeitende immer nutzen, wenn es möglich ist.

Und: Kein Passwort darf zweimal verwendet werden. Ein einzelner Diebstahl von Login-Daten ist ein eingegrenztes Problem. Wer hingegen immer das gleiche Passwort nutzt, gewährt Dieben Zugriff zu sämtlichen Accounts.

3. Keine Anhänge, keine externen Links

Eine der einfachsten Methoden, um Phishing-Angriffen und Malware zu begegnen, ist, dass Mitarbeitende Links und Anhänge in E-Mails nicht einfach so öffnen dürfen. Möglich wird dies durch strikte technische Begrenzungen. Administratoren können auch Warnhinweise integrieren, die Mitarbeitende vor dem Öffnen bestätigt müssen.

4. Updates zügig aufspielen

Sicherheitslücken in Software sind häufig. In vielen Fällen ist es möglich, sie nach ihrer Entdeckung schnell zu beheben. Doch bis das neue Update aufgespielt ist, besteht ein erhöhtes Risiko, über solche Lücken attackiert zu werden. Dementsprechend ist es Voraussetzung für eine gute Sicherheitspolitik, dass Patches zügig aufgespielt werden.

Doch nicht immer halten sich Mitarbeitende daran, die Updates zügig durchzuführen. Dann hilft eine Lösung wie MDM, bei der es möglich ist, das Gerät aus der Ferne zu warten. Die IT kann dadurch dazu beitragen, dass die gesamte im Unternehmen genutzte Software auf dem aktuellen Stand ist.

5. Keine öffentlichen Hotspots

Smartphones, über die Zugang zu Firmendaten besteht, sollten niemals über öffentliche Hotspots betrieben werden. Sie sind ein Einfallstor für Malware wie Trojaner. Ähnliches gilt übrigens auch für Bluetooth: Der Empfang von Dateien aus unbekannten Quellen sollte in den Sicherheitsrichtlinien untersagt sein.

6. Technologisch sichere Apps nutzen

Schon kleine Programme können ein enormes Sicherheitsrisiko darstellen. Deswegen sollten Mitarbeitende Apps nur aus den Software-Stores herunterladen, also niemals inoffizielle Quellen nutzen. Zudem sollten Sie die Berechtigungen beachten und bei unnötigen Zugriffsanforderungen zu Alternativen greifen. Ebenfalls wichtig ist das regelmäßige Update der Programme. Über den Versionenverlauf lässt sich leicht herausfinden, welche Programme gut gepflegt werden.

7. Datenschutz beachten

Nicht jede App ist mit den Datenschutzgesetzen vereinbar. Unternehmen müssen die Nutzung solcher Apps untersagen. Bei der Mischnutzung sollten Container und unterschiedliche Nutzungsprofile eingesetzt werden, um Datenschutzverstöße zu verhindern.

8. Gerät immer im Auge behalten

Mitarbeitende sollten ihr Smartphone immer im Auge behalten und im Optimalfall am Körper mit sich führen. Auf diese Weise sind sie kein leichtes Ziel für Diebe, die das Smartphone und mit ihm die enthaltenen Daten entwenden. Außerdem darf ein Smartphone niemals frei zugänglich sein, sondern sollte durch sichere Passwörter geschützt sein.

Die Lösung für viele Sicherheitsprobleme: MDM

Viele Risiken lassen sich mittels MDM deutlich verringern. So können aktuelle Updates auch aus der Ferne aufgespielt werden. Die Installation von unsicheren Apps kann MDM ebenfalls verhindern. Ferner besteht die Möglichkeit, die Daten für die geschäftliche Nutzung noch einmal gesondert abzusichern, sodass der Sicherheitsstandard trotz Mischnutzung jederzeit hoch ist.

Fazit

Keine Führungskraft sollte die Wichtigkeit einer sicheren Nutzung von Smartphones unterschätzen. Schon kleinere menschliche Fehler können Cyberkriminellen Tür und Tor öffnen und Millionenschäden verursachen. Es gibt jedoch diverse Möglichkeiten, die Risiken und Schäden deutlich zu verringern. Vor allem MDM stellt hier ein sehr leistungsstarkes Werkzeug dar.

Wie können Datenlecks auf dem Handy entstehen?

Eine typische Ursache für Datenlecks sind Apps, die umfangreiche Berechtigungen fordern und Daten auf ihre eigenen Server übertragen.

Ist Cyber-Security wichtig?

Cybercrime verursacht jährlich Schaden in Millionenhöhe und kann jedes Unternehmen oder auch Privatperson treffen. Die Zahl der Angriffe steigt zudem, sodass Cyber-Security nicht nur wichtig ist, sondern auch immer relevanter wird.

Wie gelangt ein Virus auf das Handy?

Ein Smartphone bietet viele Einfallstore für Viren und andere Malware: E-Mails, freie Hotspots, Bluetooth, SMS, MMS und Downloads sind die häufigsten Ursachen.