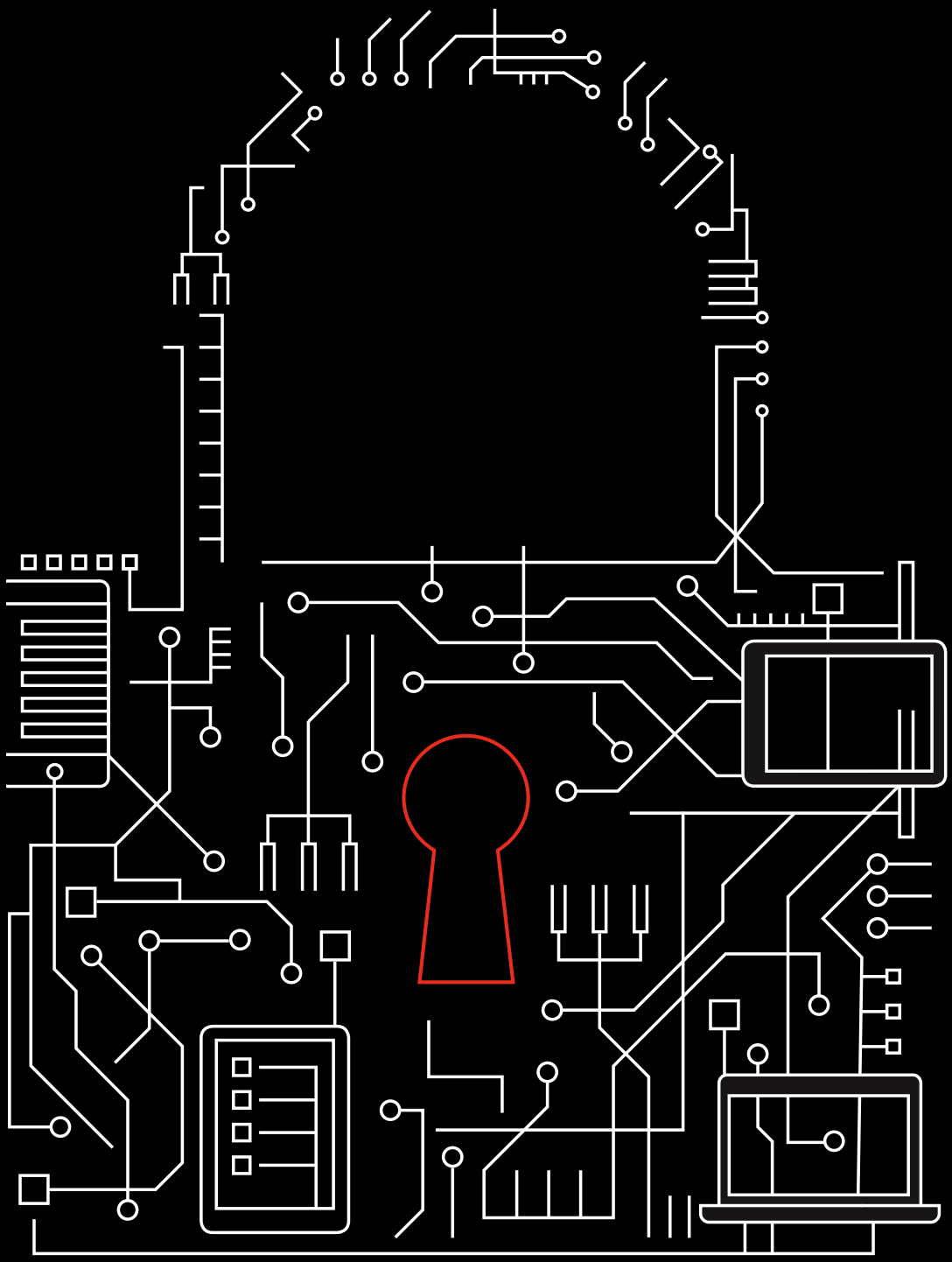
Mobile Security Index

2020
Kurzfassung



verizon

Innovation braucht Mobilgerätesicherheit

Moderne Unternehmen müssen innovativ sein, um zu überleben. Damit ist heute auch Mobilgerätetechnologie gemeint.

Für unseren Mobile Security Index 2020 haben wir die Umfrageteilnehmer unter anderem gebeten, auf einer Skala von 1 bis 10 anzugeben, wie wichtig die Mobilgerätesicherheit für ihr Unternehmen ist. 83 % der Antworten lagen zwischen 8 und 10. Sie sehen die Mobilgerätesicherheit also nicht mehr als Extra, sondern als Grundvoraussetzung für den Schutz zukünftiger Innovationen und Transformationen. Auch die Normen und Vorschriften rund um den Datenschutz werden immer strenger – nicht zuletzt, weil sowohl Geschäfts- als auch Privatkunden immer sicherheitsbewusster und anspruchsvoller werden.

Angetrieben wird all das vom ständigen Wettlauf mit Cyber-Kriminellen, die zum Teil ebenfalls sehr innovativ sind. Anders ausgedrückt: Die Mobilgerätesicherheit ist eine unaufhörliche Herausforderung, die sich mit den richtigen Tools allein nicht bewältigen lässt. Sie brauchen zudem einen Ansatz, der die Mobilgerätesicherheit zu einer Kernkomponente Ihrer IT-Strategie macht.

Deshalb möchten wir Ihnen mit diesem Dokument einen Überblick über den Stand der Technik und die Bedrohungen vermitteln, mit denen Unternehmen derzeit konfrontiert sind.

54 %

54 % der Umfrageteilnehmer haben weniger Vertrauen in die Mobilgerätesicherheit als in die Sicherheit ihrer anderen Systeme.

verizon

Mehr Unternehmen werden zu Opfern

Das vielleicht beunruhigendste Ergebnis des diesjährigen Mobile Security Index ist leider keine große Überraschung: Der Anteil der Unternehmen, die bereits mindestens einen Sicherheitsvorfall zu verzeichnen hatten, nimmt weiter zu. Seit unserem ersten Bericht im Jahr 2018 ist er um 41 % gestiegen. Hacker haben schon früh erkannt, dass immer mehr Unternehmen mobiles Arbeiten – und den Zugriff auf wertvolle Daten von Mobilgeräten aus – unterstützen und sie haben schnell Mittel und Wege gefunden, das auszubeuten.

Dazu gehören neben bewährten Taktiken wie Phishing und Malware auch raffinierte neue Tricks. Betroffen sind alle Komponenten des mobilen Ökosystems, von Nutzern und Anwendungen bis hin zu Geräten und Netzwerken.

Anteil der infiltrierten Unternehmen

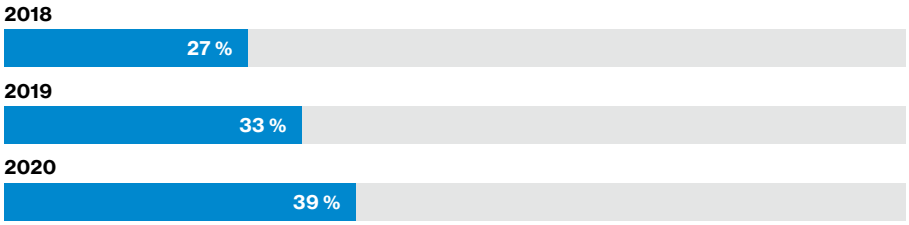


Abbildung 1: Gab es in Ihrem Unternehmen im vergangenen Jahr einen oder mehrere Sicherheitsvorfälle, bei denen Mobilgeräte oder Geräte im Internet der Dinge infiltriert wurden?

Nutzer

Die Nutzer sind seit jeher eine Herausforderung, wenn es um die IT-Sicherheit geht. Manche missachten Sicherheitsrichtlinien absichtlich, andere lassen versehentlich Sicherheitslücken entstehen und wieder andere wollen sich auf Kosten des Unternehmens bereichern. Das wissen auch Angreifer – und sie nutzen es aus. Zu den bewährtesten Angriffsformen gehört das Social Engineering,

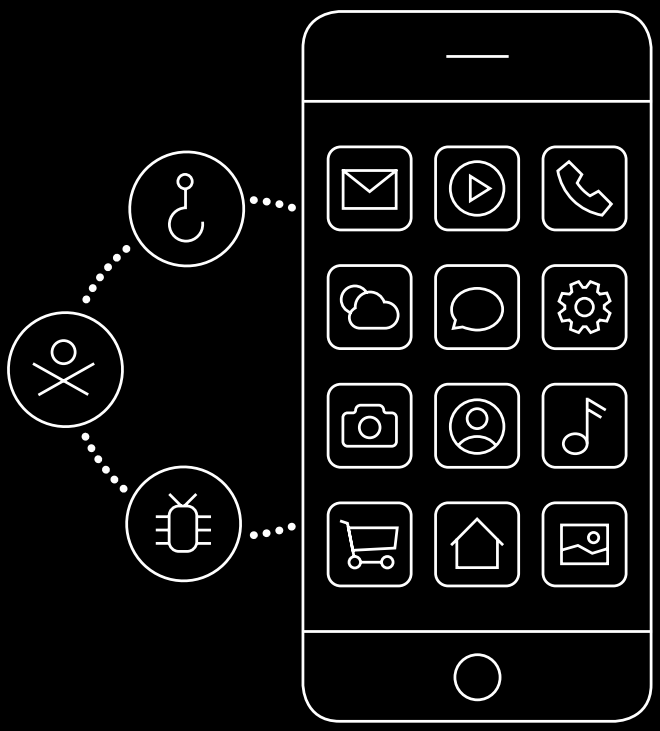
insbesondere in Form von Phishing und CEO Fraud. Letzteres wird auch als BEC (Business Email Compromise) bezeichnet und führt laut einem aktuellen Bericht eines US-Geheimdienstes zu Schäden in Höhe von fast 130.000 US-Dollar pro erfolgreichem Angriff. Zum Vergleich: Bei einem Banküberfall liegt der durchschnittliche Schaden bei 3.000 US-Dollar.[1]

Es gibt kein Allheilmittel für den Schutz von Mobilgeräten, doch Richtlinien zu ihrer akzeptablen Nutzung können ein guter erster Schritt sein – vorausgesetzt, dass die Mitarbeiter über die drohenden Gefahren und die Richtlinien informiert werden. Eine gute Richtlinie enthält Kriterien zur Erkennung akzeptabler und inakzeptabler Websites, setzt Rahmen für akzeptable Datenvolumen und beschreibt, was in puncto Compliance von den Mitarbeitern erwartet wird. Damit leistet sie einen wichtigen Beitrag zum Schutz der Unternehmensdaten. Wir mussten bei unserer Umfrage jedoch leider feststellen, dass es in 44 % der untersuchten Unternehmen keine solche Richtlinie gibt.

15 %

15 % der Unternehmenskunden erhielten im 3. Quartal 2019 mindestens einen Phishing-Link auf einem Mobilgerät. (In den USA waren es 18 %.)

Sie möchten strengere Richtlinien für die akzeptable Nutzung formulieren? Lesen Sie unseren Leitfaden zu diesem Thema. ›



Wenn die Hacker den Innovationspreis gewinnen

Bei unseren Untersuchungen haben wir in diesem Jahr Beweise dafür gefunden, dass Hacker schädliche Apps in offizielle App Stores geschmuggelt hatten und Tarnmethoden wie verzögerte Trigger und eigens entwickelte Fonts nutzten, damit schädliche E-Mail-Inhalte nicht von Scan-Software erkannt werden konnte.

21 %

Bei 21 % der Unternehmen, die einem Angriff zum Opfer gefallen waren, hatte eigenen Angaben zufolge eine unbefugt bzw. ohne Genehmigung genutzte App den Angriff begünstigt.

Anwendungen

Ransomware und andere Malware sind nach wie vor gefährlich und weit verbreitet. Darüber hinaus breiten sich auch Methoden wie das Cryptojacking (also der Missbrauch infiltrierter Geräte zum Schürfen von Cyber-Währungen wie Bitcoins) immer weiter aus. Für den legitimen Besitzer bedeutet das im besten Fall, dass der Akku sehr schnell leer ist. Es kann aber auch zu anderen Störungen und sogar zum Ausfall des Geräts führen.

In diesem Jahr beschrieben die Befragten in 86 % der untersuchten Unternehmen sich als besorgt über Malware. Dennoch schreiben die meisten Unternehmen ihren Mitarbeitern nicht vor, welche Anwendungen sie nutzen dürfen und welche nicht. Nur in 43 % der untersuchten Unternehmen sind ausschließlich Apps aus einem offiziellen App Store oder aus dem App Store des Unternehmens selbst erlaubt.

Geräte

Für unseren diesjährigen Bericht haben wir ein breites Spektrum von Unternehmen untersucht, von Firmen mit weniger als 100 Mobilgeräten bis zu Großkonzernen mit über 10.000. Überall wurden die gleichen Sorgen genannt, von verlorenen Geräten bis hin zu Schwachstellen in deren Betriebssystemen. Der Verlust oder Diebstahl von Mobilgeräten gilt in 83 % der untersuchten Unternehmen als Anlass zur Sorge und in 20 % dieser Unternehmen beschrieben die Befragten die vorhandenen Schutzmaßnahmen als unzureichend. Viele Mobilgeräte bieten allerdings Sicherheitsfunktionen als Standard, mit denen das Risiko sich erheblich reduzieren lässt, beispielsweise die Verschlüsselung der Daten auf dem Gerät und das Löschen per Fernzugriff.

Die Betriebssysteme auf Mobilgeräten geben ebenfalls Anlass zur Sorge und sind oft nicht auf dem neuesten Stand. Knapp die Hälfte (49 %) der unternehmenseigenen Geräte werden ohne Richtlinien für das Update-Manangement betrieben.

31 %

Daten von MobileIron zufolge wurden auf 31 % der Geräte bekannte Bedrohungen gefunden.[2]

2 bis 3

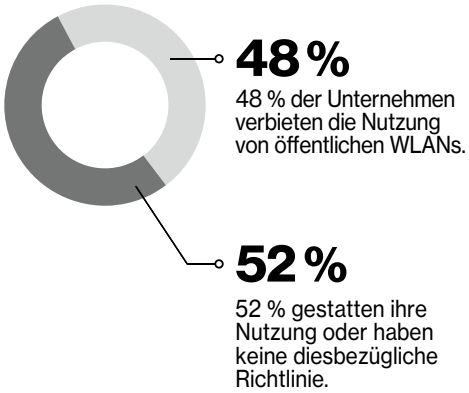
Anzahl der unsicheren WLAN-Hotspots, mit denen jedes Gerät sich pro Tag verbindet

Netzwerke

Öffentliche WLANs sind eine ständige Versuchung für Nutzer – und ein weiteres Risiko für Unternehmen. Bei 20 % der Unternehmen, deren Mobilgeräte von Hackern infiltriert worden waren, spielte eigenen Angaben zufolge ein unautorisierter oder unsicherer WLAN-Hotspot eine Rolle bei dem Angriff.

Wandera zufolge stellen Mitarbeiter im Durchschnitt Verbindungen zu 24 WLAN-Hotspots pro Woche her.[3] Laut NetMotion verbindet jedes Gerät sich im Schnitt mit zwei bis drei unsicheren WLAN-Hotspots pro Tag.[4]

Richtlinien zu öffentlichen WLANs



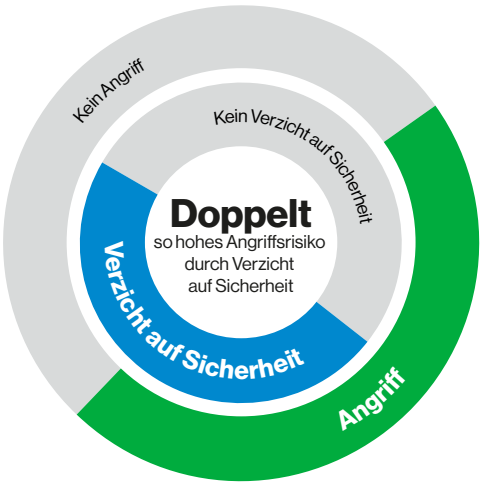
Mitarbeiter und öffentliche WLANs

Abbildung 2: Dürfen Ihre Mitarbeiter öffentliche WLANs (z. B. in einem Café oder Hotel) nutzen, um von dort aus zu arbeiten? Nutzen Sie selbst manchmal ein öffentliches WLAN für professionelle Zwecke?

Abschätzung der Auswirkungen

Man sollte meinen, dass sich längst in allen Unternehmen herumgesprochen hat, wie wichtig die Mobilgerätesicherheit für die Sicherheit der ganzen Unternehmensinfrastruktur ist. Die Beweislage ist jedoch keineswegs eindeutig. In 43 % der untersuchten Unternehmen gaben die Befragten zu, dass sie mitunter auf Mobilgerätesicherheit verzichten, um Termine einzuhalten oder Produktivitätsziele zu erfüllen. In diesen Unternehmen war die Wahrscheinlichkeit eines erfolgreichen Angriffs doppelt so hoch wie in den anderen.

Wie kommt es zu derart riskanten Entscheidungen? Schnelligkeit (62 %) und Bequemlichkeit (52 %) waren die meistgenannten Gründe, Rentabilität (46 %) folgte auf Platz drei. All das sind natürlich wichtige kommerzielle Faktoren, doch wenn man bedenkt, dass der Verzicht auf Sicherheitsmaßnahmen die Wahrscheinlichkeit eines Cyber-Angriffs verdoppelt, wird es deutlich schwieriger, ihn zu rechtfertigen.



Verzicht und Verstoß

43 %

43 % der Unternehmen verzichteten auf Sicherheit.

39 %

Bei 39 % der Unternehmen kam es zu einem Sicherheitsverstoß.

Abbildung 3: Gab es in Ihrem Unternehmen im vergangenen Jahr einen oder mehrere Sicherheitsvorfälle, bei denen IoT- oder Mobilgeräte involviert waren? Hat Ihr Unternehmen jemals auf Mobilgerätesicherheit oder den Schutz von IoT-Geräten verzichtet, um ein Projekt rechtzeitig abzuschließen?

Gravierende Auswirkungen

In 66 % der Unternehmen, die einem Angriff zum Opfer gefallen waren, beschrieben die Befragten die Auswirkungen als „bedeutend“. Zudem beschrieben 37 % der Befragten die Schadensbehebung als schwierig und teuer.

Die Auswirkungen dieser Angriffe gingen oft weit über die Mobilgeräte hinaus. Zu den unmittelbaren Konsequenzen gehörten:

- Ausfälle (59 %)
- Datenverlust (56 %)
- Bußgelder(29 %)

Wenn Sie nach all dem immer noch glauben, dass Ihr Unternehmen nicht gefährdet sei, weil es zu klein ist oder weil Cyber-Angriffe in Ihrer Branche kein Thema sind, haben wir schlechte Nachrichten für Sie. Wir haben keine einzige Branche gefunden, in der es keine Cyber-Angriffe gab und unter den Opfern waren sowohl Kleinunternehmen mit weniger als 50 Mitarbeitern als auch Großkonzerne mit über 10.000.

Auswirkungen eines Angriffs

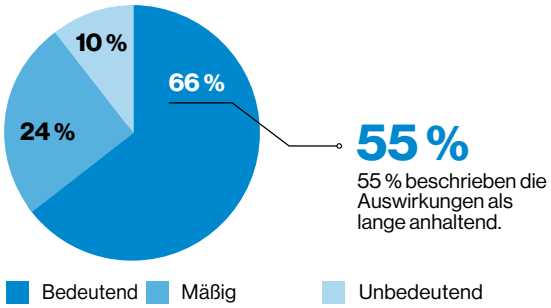


Abbildung 4: Beantworten Sie diese Fragen nur, wenn Ihr Unternehmen mindestens einem Angriff zum Opfer gefallen ist: Wie schwerwiegend waren die Auswirkungen? Falls die Auswirkungen erheblich waren: Gab es langfristige Konsequenzen?

Ausblick: Cloud, IoT und 5G

Durch eine noch intensivere Nutzung von Clouds, IoT-Geräten und 5G-Netzwerken werden in Zukunft völlig neuartige Kunden- und Mitarbeitererlebnisse möglich sein, die Unternehmen in allen Sektoren grundlegend verändern werden. Deshalb werden diese drei Technologien und ihre Auswirkungen auf die Mobilgerätesicherheit im diesjährigen Mobile Security Index genauer untersucht.

Cloud

Die steigende Bedeutung von Clouds in Infrastrukturen kann nicht überschätzt werden. In 57 % der untersuchten Unternehmen wird mehr als die Hälfte der neu erfassten oder generierten Unternehmensdaten in der Cloud gespeichert. 84 % sind „zunehmend" auf in der Cloud gespeicherte Daten angewiesen. Dennoch blockiert nur etwa die Hälfte (52 %) die Nutzung von Cloud-Apps, wenn über unbekannte Netzwerke auf sie zugegriffen wird.

Internet der Dinge (IoT)

Um das IoT genauer zu betrachten, haben wir diejenigen Umfrageteilnehmer identifiziert, die für die Anschaffung, Verwaltung oder Sicherung von IoT-Geräten verantwortlich sind und sie gebeten, einige zusätzliche Fragen zu beantworten. Dabei stellte sich heraus, dass IoT-Umgebungen dieselben Herausforderungen präsentieren, die wir schon bei Mobilgeräten gesehen hatten. Fast ein Drittel (31 %) unserer IoT-Gruppe gab zu, einem Angriff zum Opfer gefallen zu sein, bei dem ein IoT-Gerät infiltriert wurde. Auch hier hatte zu große Hast Angreifern in einigen Fällen Vorschub geleistet. 41 % gaben zu, auf IoT-Sicherheit verzichtet zu haben, „um ein Projekt fertigzustellen" – mit negativen Konsequenzen. In Unternehmen, die das IoT nutzten, aber auf IoT-Sicherheitsmaßnahmen verzichtet hatten, war die Wahrscheinlichkeit eines Angriffs, bei dem mindestens ein IoT-Gerät infiltriert wurde, 1,7-Mal höher.

5G

5G verspricht fesselnde neue interaktive Services, wie Augmented und Virtual Reality. Darüber hinaus wird erwartet, dass 5G die Entwicklung von IoT-Anwendungen wie verbundenen Fahrzeugen, intelligenten Gebäuden, Smart Citys und anderen „intelligenten Räumen" beschleunigen wird. Vorrichtungen zum Schutz dieser Services und Anwendungen sind Kernkomponenten der Architekturen, auf denen 5G basiert.

Unter anderem bietet 5G die folgenden neuen Sicherheitsfunktionen:

- Besserer Schutz vor unbefugtem Tracking und Identitätsdiebstahl mithilfe von permanenten, versteckten Abonnement-IDs und weltweit eindeutigen, temporären IDs (Subscription Concealed Identifier, SUCI und Globally Unique Temporary Identifier, 5G GUTI)
- Stärkere Resilienz gegen Angriffe durch die Nutzung von softwaredefinierten Netzwerken (SDN) und virtualisierten Netzwerkfunktionen (NFV)
- Maßgeschneiderte Sicherheit zur Unterstützung neuer Geräte und Anwendungsbereiche
- Besserer Schutz vor unautorisierten Base Stations durch die Nutzung impliziter Schlüssel und konsequente Verifizierung bei der Nutzung von WLAN und anderen Netzwerken, die nicht dem 3GPP-Standard entsprechen

Was treibt diese Änderungen voran?

Regierungen in aller Welt verschärfen vorhandene oder erlassen neue Bestimmungen hinsichtlich der Mobilgerätesicherheit. In 67 % der untersuchten Unternehmen waren striktere Vorschriften ein Grund dafür, dass mehr für die Sicherheit ausgegeben wurde.

Vielerorts wird die Mobilgerätesicherheit leider erst ernst genommen, wenn sie versagt hat. 43 % der Unternehmen, die einem Angriff zum Opfer gefallen waren, hatten das Budget für die Mobilgerätesicherheit für das kommende Jahr erheblich aufgestockt – im Vergleich zu nur 17 % der Unternehmen, die nicht angegriffen worden waren.

84 %

84 % der Unternehmen sind zunehmend von in der Cloud gespeicherten Daten abhängig.

31 %

31 % der Teilnehmer, die wir zum IoT befragten, hatten bereits einen Angriff erlebt, bei dem ein IoT-Gerät infiltriert wurde.

Unternehmen, die einen Angriff erlitten hatten, neigten dazu, deutlich mehr für die Sicherheit auszugeben.

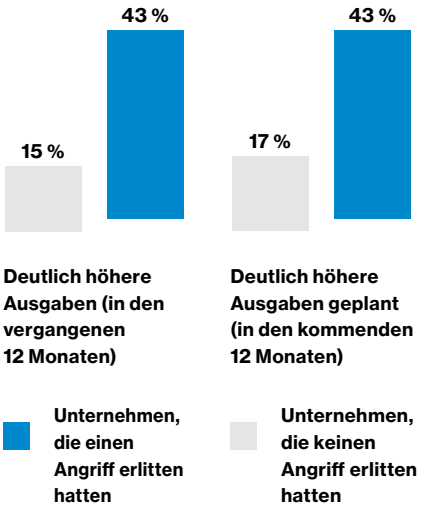
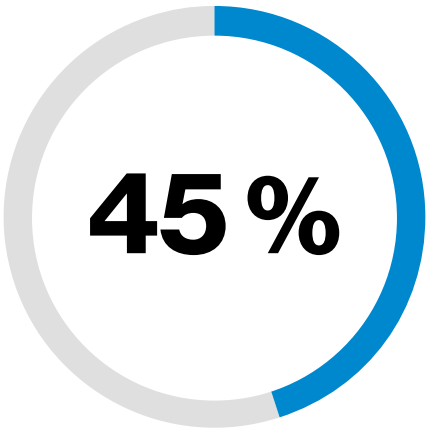


Abbildung 5: Auswirkungen eines Angriffs auf das Budget für die Mobilgerätesicherheit

So verbessern Sie die Mobilgerätesicherheit

45 Prozent der Befragten glauben, dass ihre Abwehrmaßnahmen nicht mit den sich ständig weiterentwickelnden Fähigkeiten der Angreifer Schritt halten. Nutzen Sie den Mobile Security Index 2020, um nicht zu diesen 45 % zu gehören! In diesem Jahr haben wir Interviews mit Experten in unseren Bericht aufgenommen, die detaillierte Empfehlungen für die Verbesserung und individuelle Anpassung von Sicherheitsansätzen enthalten.

Im Folgenden geben wir Ihnen als kleinen Vorgeschmack einen Überblick über die Top-Tipps zur Verbesserung der Mobilgerätesicherheit.



In 45 % der Unternehmen bezweifeln die Befragten, dass ihre Sicherheitsmaßnahmen mit den steigenden Fähigkeiten von Hackern Schritt halten.

Nutzer

- Erstellen Sie offizielle Richtlinien für die akzeptable Nutzung von Mobilgeräten. Diese sollten festlegen, welche Verantwortung Mitarbeiter übernehmen, wenn sie Privatgeräte für die Arbeit nutzen (Stichwort „Bring your own Device“), welche Netzwerke Mitarbeiter nutzen und welche Apps sie installieren dürfen.
- Räumen Sie der Sicherheit oberste Priorität ein, sensibilisieren und schulen Sie alle Mitarbeiter regelmäßig und sorgen Sie dafür, dass alle Nutzer wissen, wie Verdacht erregende Beobachtungen zu melden sind.
- Erstellen Sie Richtlinien für die Stärke und Wiederverwendung von Passwörtern und die Nutzung der Zweifaktorauthentifizierung. Sorgen Sie dafür, dass alle Nutzer diese Richtlinien kennen und einhalten.

Anwendungen

- Beschränken Sie den Zugriff auf Daten auf das unbedingt erforderliche Mindestmaß.
- Gestatten Sie nur die Installation von Apps, die aus überprüften Quellen stammen. Blockieren Sie alle aus dem Internet heruntergeladenen Apps.
- Sorgen Sie dafür, dass alle Patches zeitnah eingespielt werden.

Geräte

- Ändern Sie alle vom Anbieter definierten und Standardpasswörter und verwenden Sie Passwörter nicht wieder.
- Implementieren Sie Richtlinien für das Sperren und Isolieren anfälliger, infizierter und verlorener bzw. gestohlener Geräte.
- Nutzen Sie eine Lösung für das Mobilgeräte-Management (Mobile Device Management, MDM), um das Patch-Management zu vereinfachen und Ihre Richtlinien für die akzeptable Nutzung und die Authentifizierung durchzusetzen.
- Besorgen Sie sich Software für die Bedrohungserkennung auf Mobilgeräten und durchsuchen Sie Ihre Geräte regelmäßig nach Schwachstellen.

Netzwerke

- Verschlüsseln Sie alle Daten, die über ungesicherte Netzwerke übertragen werden.
- Informieren Sie Ihre Mitarbeiter über die mit öffentlichen WLANs einhergehenden Gefahren und blockieren Sie Verbindungen zu unbekannten oder unsicheren WLANs.
- Erwägen Sie einen Zero-Trust-Ansatz.

Cloud-Services

- Schränken Sie die Nutzung ungeprüfter Cloud-Anwendungen und insbesondere die Nutzung von Dateifreigabe-Plattformen ein.
- Der Zugriff auf Cloud-Services sollte nur über vertrauenswürdige Netzwerke oder VPNs möglich sein.

Holen Sie sich den Bericht – zum Schutz Ihres Unternehmens

Sie haben den ersten Schritt zur Verbesserung der Mobilgerätesicherheit getan. Laden Sie als Nächstes den vollständigen „Mobile Security Index (MSI) 2020“ herunter. Unternehmen wie Ihres können eine effektive, mehrschichtige Sicherheitsinfrastruktur für das mobile Arbeiten einrichten – und wir haben Tools im Angebot, die Sie dabei unterstützen.

MSI 2020: Hauptbericht

Im vollständigen Mobile Security Index 2020 finden Sie noch mehr detaillierte Statistiken und Analysen der Gefahren für Mobilgeräte sowie Interviews mit einem Bereichsleiter des US-amerikanischen FBI, dem CISO von Verizon und anderen Sicherheitsexperten.

MSI 2020: Tool für die Sicherheitsbewertung

Bewerten Sie die Mobilgerätesicherheit in Ihrem Unternehmen mit unserem Tool! Anschließend erhalten Sie einen individuell angepassten Bericht, der Ihr Sicherheitsniveau mit dem ähnlicher, für MSI 2020 untersuchter Unternehmen vergleicht und Empfehlungen für Verbesserungen enthält.

MSI 2020: Leitfaden für Richtlinien zur akzeptablen Nutzung

In diesem interaktiven Leitfaden wird erklärt, was starke Richtlinien zur akzeptablen Nutzung auszeichnet und wie Sie solche Richtlinien erstellen oder Ihre vorhandenen Richtlinien verbessern.

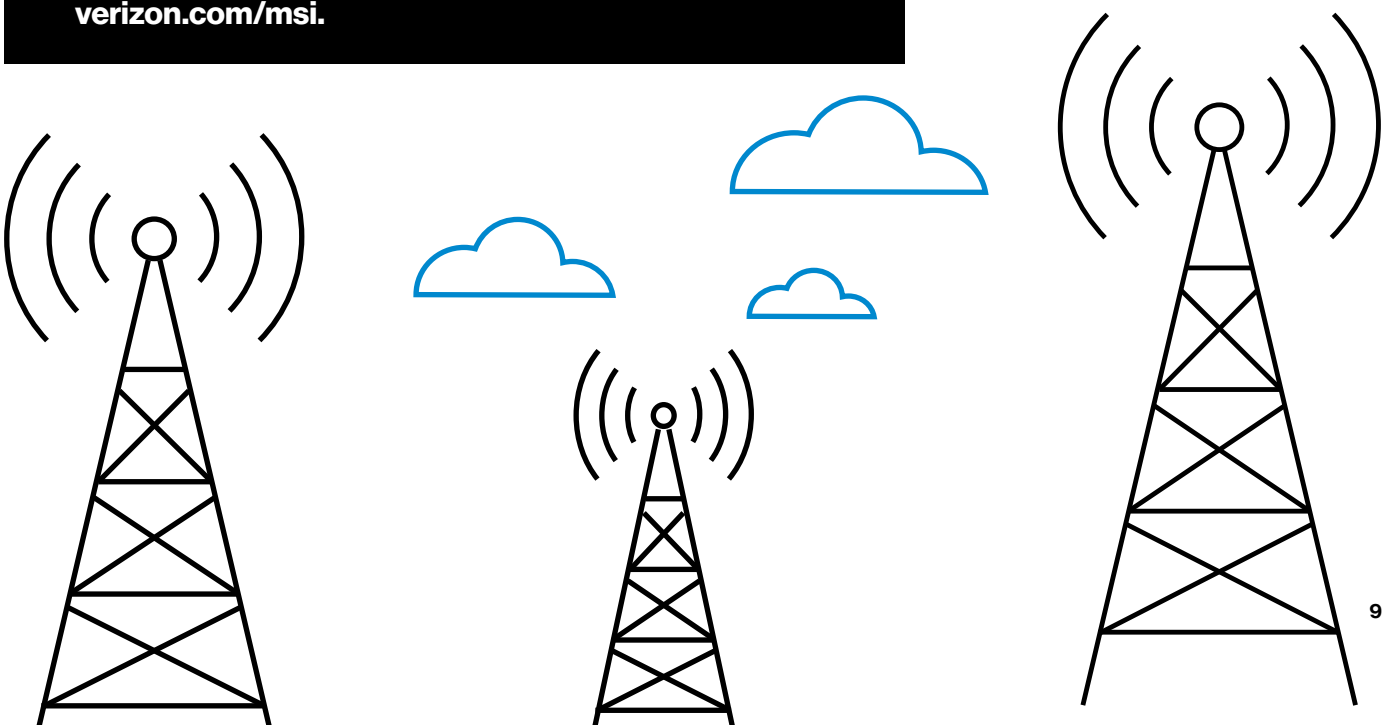
MSI 2020: Branchenspezifische Berichte

Mit diesen Berichten gehen wir ausführlicher auf den Stand der Mobilgerätesicherheit und die spezifischen Risiken im Finanzwesen, im Gesundheitswesen, im Einzelhandel, in der Fertigung und im öffentlichen Dienst ein. Zudem werfen wir einen Blick auf kleine und mittlere Unternehmen.

Video: Interview zur Mobilgerätesicherheit

Sie möchten wissen, wie wir bei Verizon die Mobilgerätesicherheit im eigenen Haus handhaben? In diesem Video beschreiben wir unseren mehrschichtigen Ansatz für die Mobilgerätesicherheit.

Weitere Informationen finden Sie unter enterprise.verizon.com/msi.



verizon

[1] Christopher McMahon, U.S. Secret Service
[2] Diese Angabe basiert auf von MobileIron bereitgestellten aggregierten Nutzungsdaten für 2019.
[3] Diese Angabe beruht auf Daten von Wandera Threat Research für den Zeitraum von November 2018 bis Oktober 2019.
[4] Im Durchschnitt stellt ein typisches Mobilgerät Verbindungen zu zwei bis drei unsicheren WLAN-Hotspots pro Tag her. NetMotion zufolge geschieht das am häufigsten an Standorten im Einzelhandel, Hotel- und Gaststättengewerbe sowie an Flughäfen und anderen Verkehrsknotenpunkten.