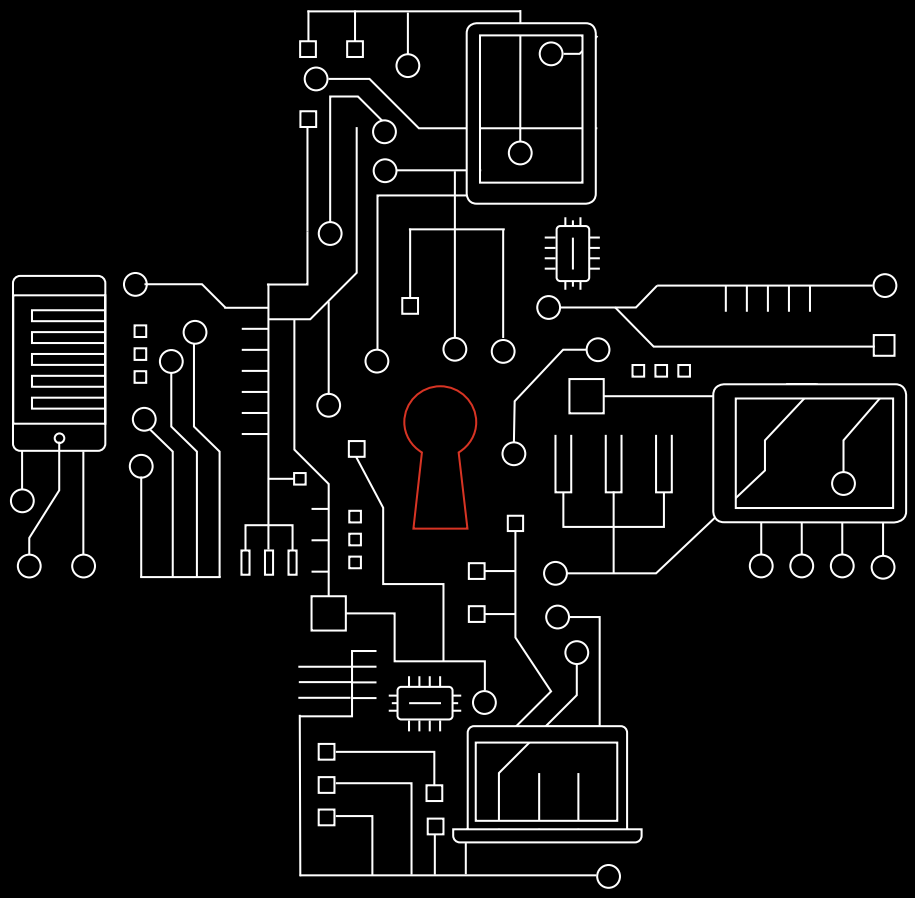
# Mobile Security Index 2020

## Blickpunkt Gesundheitswesen

Ein detaillierter Überblick über die Sicherheit von Mobilgeräten in medizinischen Behandlungs- und Versorgungszentren, Krankenhäusern und Pflegeheimen.



verizon

# Bieten Sie Ihren mobilen Nutzern effektiven Schutz?

## Unternehmen aus dem Gesundheitswesen können durch den Einsatz von Mobilgeräten beträchtliche Vorteile erzielen, sollten dabei aber nicht vergessen, dass sie über große Mengen sensibler Daten verfügen, die ein lukratives Ziel für Cyber-Kriminelle sind. Nur mit effektiven Maßnahmen für die Mobilgerätesicherheit können sie ihre Daten und kritischen Systeme effektiv schützen.

**88 %**

**der befragten Gesundheitsdienstleister geben an, in wachsendem Maße auf in der Cloud gespeicherte Daten angewiesen zu sein.**

Mobilgeräte können sich in der Gesundheitsbranche als wahre Lebensretter erweisen. Sie versetzen das Personal in die Lage, medizinische Daten schnell einzusehen und an Kollegen weiterzuleiten, und ermöglichen darüber hinaus eine verbesserte Überwachung und Nachbetreuung ambulanter Patienten, was sich unter anderem in einer geringeren Wiedereinlieferungsquote niederschlagen kann. Außerdem können die mithilfe von Mobilgeräten erfassten Daten als Grundlage für Analysen zur Verbesserung der Präzision von Diagnosen und Behandlungen genutzt werden. All diese Vorteile fallen noch weitaus größer aus, wenn der Einsatz von Mobilgeräten mit der Nutzung cloudbasierter Services kombiniert wird. Vor diesem Hintergrund ist es durchaus vielversprechend, dass 88 % der untersuchten Einrichtungen des Gesundheitswesens zunehmend auf in der Cloud gespeicherte Daten angewiesen sind.

**Wir haben ein unabhängiges Forschungsinstitut mit der Befragung von leitenden, für die Beschaffung, Verwaltung und Sicherung von Mobilgeräten zuständigen Fachleuten beauftragt. Insgesamt haben sich 876 Personen aus der Zielgruppe an dieser Studie beteiligt, von denen 9 % für Einrichtungen des Gesundheitswesens (wie Krankenhäuser, Behandlungszentren, Ambulanzen und Pflegeheime) tätig waren. Sofern nicht anders angegeben stammen alle hier präsentierten Daten aus dieser Umfrage.**

verizon

## Fast zwei Fünftel der Befragten waren von einem Angriff betroffen.

In 38 % der erfassten Einrichtungen gab es im vergangenen Jahr laut eigenen Angaben mindestens eine Sicherheitsverletzung im Zusammenhang mit Mobilgeräten. Das ist ein signifikanter Anstieg im Vergleich zum Vorjahreswert von 25 %.

Dieser Trend ist besorgniserregend, da hier viel auf dem Spiel steht. Einrichtungen des Gesundheitswesens verfügen über hochgradig sensible Patienten- und Mitarbeiterdaten, die Cyber-Kriminelle anziehen, weil sie sich auf dem Schwarzmarkt verkaufen oder zur Erpressung von Lösegeldern missbrauchen lassen.

So wurde der britische National Health Service (NHS) im Jahr 2017 zum Ziel eines Ransomware-Angriffs, der in Krankenhäusern im ganzen Land für Chaos sorgte. Tausende Arzttermine und Operationen mussten abgesagt oder in andere Kliniken verlegt werden.[1] Ähnlich weitreichende Folgen hatte ein Hackerangriff auf ein US-amerikanisches, auf den medizinischen Bereich spezialisiertes Inkassounternehmen im Jahr 2019, bei dem Kundendaten von über 20 Kliniken, Diagnoselaboren und anderen Gesundheitsdienstleistern gestohlen wurden. Insgesamt waren fast 25 Millionen Menschen betroffen.[2]

Angesichts der potenziellen Auswirkungen derartiger Vorfälle auf Patienten und Mitarbeiter ist es überaus erstaunlich, dass 37 % der Befragten aus dem Gesundheitswesen zugeben, den Schutz von Mobilgeräten zugunsten eines schnellen Abschlusses von Modernisierungsinitiativen vernachlässigt zu haben. Genau wie in anderen Branchen hat dies auch hier drastische Konsequenzen. Gesundheitsdienstleister, die bei der Sicherheit von Mobilgeräten Kompromisse eingehen, werden mit einer 1,9-mal höheren Wahrscheinlichkeit Opfer eines Angriffs.


**36 % der Umfrageteilnehmer aus dem Gesundheitswesen, deren mobile Nutzer im vergangenen Jahr zum Ziel eines Angriffs wurden, berichteten von massiven Auswirkungen.**




**37 %**

**der Gesundheitsdienstleister haben die Sicherheit zugunsten anderer Prioritäten vernachlässigt.**

**38 %**

**der erfassten Einrichtungen des Gesundheitswesens haben im vergangenen Jahr laut eigenen Angaben mindestens einen Angriff auf Mobilgeräte festgestellt.**

Abbildung 1: Ist in Ihrer Einrichtung im vergangenen Jahr eine Sicherheitsverletzung aufgetreten, von der Mobilgeräte oder IoT-Geräte betroffen waren? Wurde die Sicherheit von Mobilgeräten (einschließlich IoT-Geräten) in Ihrer Einrichtung schon einmal hintangestellt, um Modernisierungsinitiativen schneller abzuschließen?

**71 %**

**der Einrichtungen wurden durch neue gesetzliche Regelungen zu einer Neubewertung der im Zusammenhang mit der Nutzung von Mobilgeräten auftretenden Risiken veranlasst.**

**1.300**

**Laut Angaben von Netskope werden in Unternehmen durchschnittlich knapp 1.300 verschiedene Apps und Cloud-Services genutzt. 95 % davon werden nicht durch die IT-Abteilung verwaltet und überwacht.[3]**

## Die größten Sorgen der Sicherheitsverantwortlichen im Gesundheitswesen

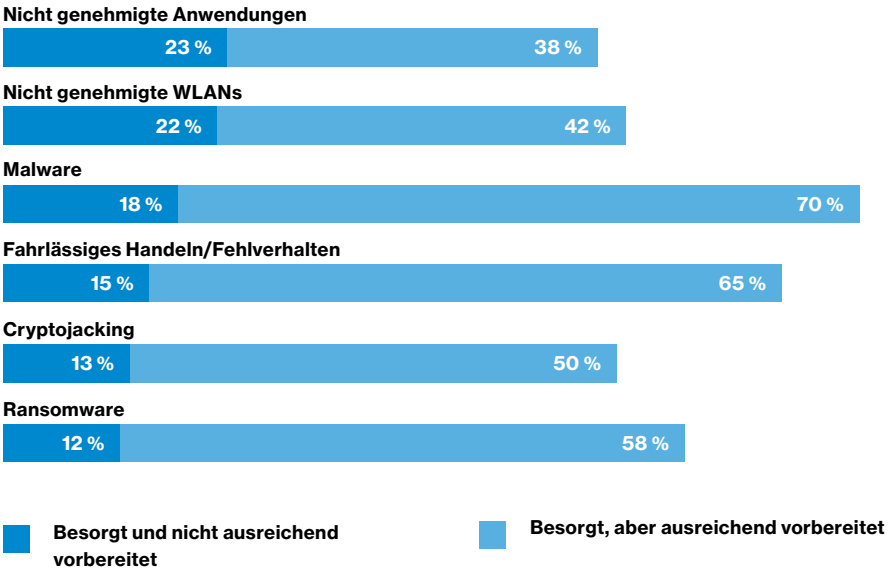



Abbildung 2: Bitte geben Sie an, wie Sie den folgenden Bedrohungen und Risiken entgegensehen.

## Die Risiken der Cloud

Mobilgeräte und die Cloud werden immer häufiger in Kombination eingesetzt. Unserer Umfrage zufolge wird der Zugriff auf cloudbasierte Services in 85 % der untersuchten Unternehmen in spätestens fünf Jahren hauptsächlich über Mobilgeräte erfolgen. Eine Mehrheit sieht in der Cloud zudem die neue Standardumgebung für die Entwicklung und Bereitstellung von Anwendungen. Darüber hinaus gaben 44 % der Teilnehmer an, dass mehr als die Hälfte ihrer neu generierten Daten in der Cloud gespeichert werden.

**Die meisten Befragten aus der Gesundheitsbranche unterschätzen die Zahl der in ihrem Unternehmen genutzten Anwendungen erheblich. 65 % meinen, dass es weniger als 100 seien. Lediglich 4 % schätzen die Zahl auf über 1000. Tatsächlich liegt sie deutlich darüber.**

## Furcht vor bekannten Gefahren

Die überwiegende Mehrheit der im Gesundheitswesen tätigen Befragten zeigte sich besorgt über die zunehmende Nutzung von Mobilgeräten: 73 % stuften das diesbezügliche Risiko in ihrer Einrichtung als moderat oder signifikant ein. Sie nannten ein breites Spektrum potenzieller Bedrohungen, darunter auch relativ neue Phänomene wie das sogenannte Cryptojacking. Am häufigsten wurden jedoch bekannte Risiken wie die Nutzung ungenehmigter Anwendungen (23 %) oder unzureichend gesicherter WLAN-Hotspots (22 %) sowie Malware-Infektionen (18 %) genannt, auf die viele Einrichtungen des Gesundheitswesens nach Meinung unserer Befragten nicht ausreichend vorbereitet seien.

Als mögliche Konsequenzen nannten die Befragten unter anderem Imageschäden (50 %) und Bußgelder (32 %). Ihre größte Sorge sind jedoch Datenverluste (62 %) und insbesondere der Diebstahl oder die Offenlegung von Patientendaten und Krankenakten. Daneben fürchten 51 % um die Sicherheit ihrer Mitarbeiterdaten, die von Cyber-Kriminellen für gezielte Phishing-Angriffe und Betrugsversuche (unter anderem zur Unterschlagung von Steuerrückzahlungen) missbraucht werden können.

## Datenverluste ohne bösen Vorsatz

Krankenakten und andere medizinische Daten werden auch in Zukunft ein lukratives Ziel für Cyber-Kriminelle sein. Dennoch bleiben Insider-Bedrohungen eine der größten Sorgen der Branche. So waren 75 % der Umfrageteilnehmer aus dem Gesundheitswesen der Meinung, dass das größte Risiko im Zusammenhang mit der Nutzung von Mobilgeräten von den eigenen Mitarbeitern ausgehe. Dennoch finden nur in 52 % der untersuchten Einrichtungen regelmäßige IT-Sicherheitsschulungen für die Mitarbeiter statt.

Dies ist einerseits bedenklich, da fahrlässiges Handeln des Personals, wie beispielsweise die Installation ungenehmigter Anwendungen oder die Nutzung unzureichend gesicherter öffentlicher WLAN-Hotspots, die Angriffsfläche vergrößert. Andererseits stellt sich die Frage, ob man von den Mitarbeitern wirklich einen größeren Beitrag zum Risikomanagement erwarten kann, wenn Entscheidungsträger den Verzicht auf Mobilgerätesicherheit zugunsten anderer Prioritäten genehmigen und diejenigen, die Sicherheitsrichtlinien erstellen, sich oft selbst nicht daran halten.

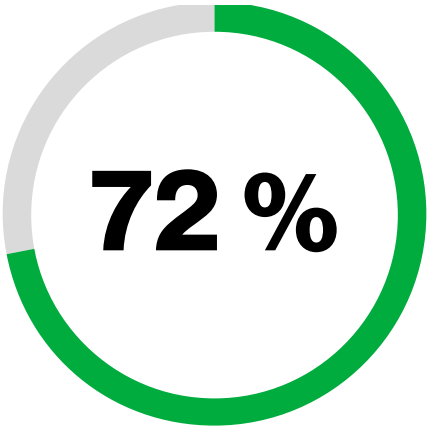
**65 %**

**der Befragten aus dem Gesundheitswesen gaben zu, dass sie öffentliche WLANs zur Erledigung von Arbeitsaufgaben nutzen, obwohl die Richtlinien dies in 23 % der Unternehmen aus dieser Gruppe explizit untersagen.**

## Gesundheitsdienstleister könnten mehr tun.

Trotz der bekannten Risiken vernachlässigen viele Gesundheitsdienstleister grundlegende Sicherheitsmaßnahmen. Nur 43 % der Befragten aus dieser Branche gaben an, dass in ihrem Unternehmen alle vorkonfigurierten oder vom Anbieter eingerichteten Passwörter systematisch geändert und sensible Daten nur in verschlüsselter Form über öffentlich zugängliche Netzwerke übertragen werden. Erweitert man diesen Kriterienkatalog um regelmäßige Sicherheitstests und die Beschränkung der Zugriffsrechte der Mitarbeiter auf das notwenige Minimum, so zeigt sich, dass nur 12 % der Gesundheitsdienstleister alle vier grundlegenden Sicherheitsmaßnahmen implementiert haben.

Des Weiteren gaben trotz der zunehmenden Cloud-Nutzung nur 35 % der Befragten aus dieser Branche an, dass ihre Unternehmen die Verwendung von cloudbasierten Anwendungen ohne Sicherheitsnachweis einschränken. Und lediglich 49 % erklärten, dass sie den Funktionsumfang geschäftlich genutzter Anwendungen reduzieren, wenn der Nutzerzugriff von einem unbekannten Netzwerk oder Standort aus erfolgt. Durch den Verzicht auf diese Vorsichtsmaßnahmen setzen sie die Daten ihrer Mitarbeiter und Patienten einem erheblichen Risiko aus.




**72 % der im Gesundheitswesen tätigen Befragten erklärten, dass sich die Implementierung effektiver Sicherheitsmaßnahmen schwierig gestaltet, da die Mitarbeiter jederzeit schnellen Zugriff auf die Unternehmensdaten benötigen.**

## Warum wird nicht mehr für die Sicherheit getan?

Als wichtigste Gründe für Kompromisse in puncto Sicherheit wurden von den Befragten betriebliche Anforderungen (64 %) und die Sicherstellung eines komfortablen Nutzererlebnisses (46 %) genannt. Das deutet darauf hin, dass viele Entscheidungsträger im Gesundheitswesen befürchten, dass stärkere Sicherheit zulasten von Produktivität und Effizienz gehen würde. In einer Branche, in der es entscheidend auf den reibungslosen Zugriff auf Daten und schnelle Entscheidungen ankommt, sind diese Sorgen durchaus berechtigt.

Wenn Sicherheitsmaßnahmen schlecht konzipiert oder unzureichend umgesetzt werden, kann sich dies nachteilig auf Mitarbeiter und Patienten auswirken. Beispielsweise könnte schon eine mangelhafte Richtlinie zur Erstellung und Erneuerung von Passwörtern die Mitarbeiterproduktivität beeinträchtigen, wachsende Supportkosten mit sich bringen (infolge einer steigenden Zahl von Zurücksetzungsvorgängen) und das Cyber-Risiko des Unternehmens vergrößern (da insbesondere bei medizinischen Notfällen starke Anreize zur Umgehung der Regeln bestehen).

**20 %**

**Laut NetMotion platzieren 20 % der mobilen Mitarbeiter restriktive IT-Sicherheitsrichtlinien ganz oben auf der Liste der frustrierendsten Hindernisse am Arbeitsplatz. „Umständliche Authentifizierungsprozesse“ belegten Rang fünf.[4]**

## Sicherheit sollte nicht zulasten der Nutzererfahrung gehen.

Vorbildlich implementierte Sicherheitslösungen können einerseits das Cyber-Risiko der Unternehmen drastisch reduzieren und wirken andererseits weitgehend im Hintergrund. Das gilt unter anderem für mobile Gateways, anpassungsfähige Authentifizierungsverfahren und auf dem Zero-Trust-Prinzip basierende Netzwerkdienste, die Systeme und Daten schützen, ohne dass die Nutzer mit zahllosen umständlichen Anmeldeprozeduren behelligt werden.

# IoT-Anwendungen im Gesundheitswesen: ein Einfallstor für Bedrohungen?

Immer mehr und immer vielfältigere Drahtlosgeräte revolutionieren die Arbeit im Gesundheitswesen. So erklärte die überwiegende Mehrheit der Befragten aus dieser Branche (94 %), dass IoT-Geräten eine tragende Rolle bei der digitalen Transformation zukommt.

Beispiele für derartige Innovationen sind intelligente Arzneimittelverpackungen, die bei der planmäßigen Einnahme von Medikamenten helfen, und in Rettungswagen installierte Sensoren, die bestimmte Patientendaten schon bei der Anfahrt ins Krankenhaus übermitteln können. In diesem Zusammenhang gaben die befragten Gesundheitsdienstleister mehrheitlich an, dass sie mithilfe von IoT-Lösungen nicht nur medizinische Geräte und die Mitarbeitereffizienz (77 %), sondern auch die eigenen Gebäude (71 %) und den Gesundheitszustand von Patienten (59 %) überwachen.

Um die mit dem IoT einhergehenden Risiken näher zu beleuchten, befragten wir zusätzlich Entscheidungsträger, die in Einrichtungen des Gesundheitswesens für die Beschaffung, Verwaltung und Sicherung vernetzter Geräte zuständig sind. 77 % der Teilnehmer aus dieser Gruppe bezeichneten ihre IoT-Geräte als anfällig für Angriffe und stuften die diesbezügliche Bedrohung als moderat oder signifikant ein. Außerdem erklärten 35 %, dass bereits mindestens eine Sicherheitsverletzung im Zusammenhang mit Mobilgeräten aufgetreten sei.

Trotzdem bekannten 35 % der Umfrageteilnehmer, die IoT-Sicherheit vernachlässigt zu haben, um Modernisierungsinitiativen schneller abschließen zu können. Das wirft die Frage auf, warum diese Teilnehmer nicht mehr für die Sicherheit tun. Die häufigste Antwort lautet: betriebliche Anforderungen. Alle Befragten aus dieser Gruppe nannten Zeitdruck als einen der Gründe für ihre Entscheidung. Im Wettlauf um die Einführung der neuesten Innovationen wird die Sicherheit anscheinend oft als nachgeordneter Aspekt betrachtet. Dies lässt sich auch daran ablesen, dass 27 % die Sicherung von IoT-Geräten bei Pilotprojekten nicht als Priorität einstufen, sondern als Aufgabe ansehen, die sie „zu einem späteren Zeitpunkt in Angriff nehmen“ können.

# So sichern Sie Ihre IoT-Geräte

Glücklicherweise gibt es zahlreiche Möglichkeiten, die Sicherheit Ihrer IoT-Geräte zu stärken. Zusätzlich zu den von uns genannten Maßnahmen zum Schutz aller Mobilgeräte sollten Sie vor allem die folgenden vier Best Practices umsetzen, um Ihr Unternehmen effektiv zu sichern:

**1. Prüfen Sie vor jeder Investition die vom Anbieter bereitgestellten Sicherheitsmechanismen.**
Ganz gleich, ob Sie serienmäßig produzierte Lösungen oder Komponenten zur Erstellung eigener IoT-Geräte anschaffen: Bitten Sie den betreffenden Anbieter in jedem Fall um genaue Angaben über die implementierten Sicherheitsmaßnahmen und prüfen Sie diese auf ihre Zweckdienlichkeit und Robustheit. Achten Sie dabei insbesondere auf die Authentifizierungs- und Verschlüsselungsmechanismen sowie die Patching-Richtlinien. Und falls Sie – wie 76 % der in unserer Studie erfassten Einrichtungen – über IoT-Geräte an abgelegenen oder schwer zugänglichen Standorten verfügen, sollten Sie deren Sicherheitssysteme mit drahtlosen Updates auf dem neuesten Stand halten.

**2. Sichern Sie sämtliche Geräte, bevor Sie sie mit Ihrem Netzwerk verbinden.**
Stellen Sie zunächst sicher, dass die neuen Geräte gegen Manipulationsversuche gesichert sind.
Danach sollten Sie alle vorkonfigurierten oder vom Anbieter eingerichteten Passwörter ändern. Deaktivieren Sie außerdem sämtliche Funktionen, die Sie nicht nutzen, und blockieren Sie alle ungenutzten Ports und Protokolle.

**3. Sorgen Sie dafür, dass Unternehmensdaten nur in verschlüsseltem Zustand übertragen und gespeichert werden.**
83 % der Befragten gaben an, dass sie personenbezogene Daten erfassen und speichern. Allerdings werden diese sensiblen Datenbestände in 25 % der Unternehmen nicht verschlüsselt. Verschlüsselte Daten sind für Hacker unbrauchbar und minimieren das Risiko, dass ein Datenleck das Image Ihrer Einrichtung dauerhaft schädigt.

**4. Nutzen Sie eine IoT-Plattform.**
Wählen Sie eine IoT-Plattform aus, mit der Sie alle Geräte auf einfache Weise überwachen und verwalten können. Dadurch erhalten Sie Zugang zu Sicherheitsfunktionen, die Ihnen die Implementierung digitaler Zertifikate und die Behebung von Schwachstellen erleichtern. Zudem können Sie mit einer IoT-Plattform die Auswirkungen eines Cyber-Angriffs einschränken, indem Sie beispielsweise SIM-Karten mit bestimmten Geräten verbinden und damit verhindern, dass gestohlene SIM-Karten missbraucht werden.

**44 %**

**der befragten Anbieter von IoT-basierten Produkten und Services nutzen digitale Zertifikate, um die Sicherheit zu stärken.**

**71 %**

**der Befragten aus dem Gesundheitswesen sind der Meinung, dass das mit der Nutzung von IoT-Geräten verbundene Risiko im Laufe des letzten Jahres gestiegen ist.**

**93 %**

**der Befragten aus der Gesundheitsbranche stimmten der Aussage zu, dass Unternehmen der Sicherheit von Mobilgeräten größere Bedeutung zumessen sollten.**

## Warten Sie nicht, bis es zu spät ist.

93 % der Befragten aus der Gesundheitsbranche stimmten der Aussage zu, dass Unternehmen der Sicherheit von Mobilgeräten größere Bedeutung zumessen sollten. Und 77 % vertraten die Ansicht, dass die Gefahr für Mobilgeräte schneller steigt als das Risiko für andere Bereiche der Unternehmensinfrastruktur.

Dennoch erklärten nur 30 % der Umfrageteilnehmer, in deren Einrichtung bereits eine Sicherheitsverletzung aufgetreten war, dass die Ausgaben für den Schutz von Mobilgeräten im vergangenen Jahr deutlich gestiegen seien. Bei den Unternehmen ohne vorherige Sicherheitsverletzung lag dieser Anteil sogar nur bei 16 %.

Das lässt darauf schließen, dass sich in der Branche erst langsam ein Bewusstsein für dieses Problem entwickelt, und bietet somit durchaus Anlass zur Besorgnis.

Die Auswirkungen eines Hackerangriffs auf Mobilgeräte sind oft gravierend und weitreichend. Bei 48 % der betroffenen Einrichtungen gab es ungeplante Ausfälle und bei 39 % wurden sensible Daten gestohlen oder offengelegt. Zudem kann die Behebung eines solchen Vorfalls langwierig, schwierig und teuer sein.

Deshalb sollten Sie nicht erst bis zur Aufdeckung eines Angriffs warten, um mit der Einführung moderner Sicherheitsmaßnahmen zum Schutz Ihrer mobilen Nutzer zu beginnen. Werden Sie noch heute aktiv!

# Weitere Ressourcen


### MSI 2020 – vollständiger Bericht

Die ausführliche Version des Mobile Security Index (MSI) 2020 enthält detaillierte Zahlen und Analysen zu mobilgerätespezifischen Bedrohungen sowie Interviews mit dem Leiter einer Ermittlungseinheit des FBI, dem Chief Security Information Officer (CISO) von Verizon und anderen führenden Sicherheitsexperten.


### MSI-2020-Bewertungstool

Mit unserem auf den Ergebnissen des MSI-Berichts basierenden Online-Bewertungstool können Sie den Reifegrad Ihres Unternehmens in Bezug auf den Schutz mobiler Nutzer ermitteln. Die nach vier Dimensionen (Problembewusstsein, Risikowahrnehmung, Gefährdung und Abwehrbereitschaft) aufgeschlüsselten Ergebnisse helfen Ihnen dabei, Bereiche mit Verbesserungsbedarf zu identifizieren und gezielt zu stärken.


### MSI 2020 – Leitfaden zur Formulierung einer Acceptable Use Policy

Dieser in 10 Schritte unterteilte Leitfaden kann Ihnen dabei helfen, umfassende Nutzungsrichtlinien zu erstellen, damit Ihre Mitarbeiter genau darüber informiert sind, welche Aktivitäten mobilen Nutzern gestattet sind und welche nicht. Auf diese Weise können Sie das von Malware, Phishing-Angriffen und anderen Bedrohungen ausgehende Risiko minimieren.

# Empfehlungen

## 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 (AUP) 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.

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

# Über den Verizon Mobile Security Index

Der MSI erscheint bereits zum dritten Mal und hat sich mittlerweile als wichtige Informationsquelle etabliert. In diesem Jahr basiert er auf einer in unserem Auftrag erstellten unabhängigen Befragung von 876 Fachleuten, die in ihren jeweiligen Unternehmen für die Anschaffung, Verwaltung und Sicherung von Mobil- und IoT-Geräten zuständig sind. Außerdem haben die in Sachen Mobilgerätesicherheit führenden Experten von Asavie, IBM, Lookout, MobileIron, NetMotion, Netskope, Symantec, VMware und Wandera Vorfallsstatistiken, Nutzungsdaten und andere nützliche Informationen beigesteuert. Darüber hinaus haben wir bei der Erstellung des Berichts mit dem FBI und dem United States Secret Service zusammengearbeitet. Wir danken allen Beteiligten für ihre wertvollen Beiträge. Diese haben uns sehr dabei geholfen, ein umfassendes Bild der Bedrohungen der Sicherheit mobiler Nutzer zu zeichnen und effektive Gegenmaßnahmen aufzuzeigen.

verizon

1 „NHS ‚could have prevented' WannaCry ransomware attack", BBC, 27. Oktober 2017.
2 „AMCA Data Breach Total Nears 25M as Wisconsin Diagnostic Laboratories Confirms 115K Record Breach", HIPAA Journal, 28. August 2019.
3 Netskope Cloud Report, Netskope, August 2019, https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019
4 Employee Frustration Index, Umfrage unter 285 Nordamerikanern aus diversen Altersgruppen und mit verschiedenen Geräten, NetMotion, September 2019, https://www.netmotionsoftware.com/blog/connectivity/mobile-frustration-index