Cyber Insights von Vodafone Business

AUSGABE 2:
KENNEN SIE JEDES DEVICE, DAS IHRE MITARBEITER VERWENDEN?

Warum ein Zero-Trust-Konzept verhindert, dass Sie zu einem weiteren Angriffsziel für Hacker werden.

Finden Sie mehr heraus

Together we can
vodafone
business

Contents

Die zweite Ausgabe unseres vierteljährlich erscheinenden eBooks zu Cyber Insights soll Ihnen dabei helfen, mit der sich ständig ändernden Situation der Cyberrisiken Schritt zu halten.

In dieser Ausgabe setzen wir unser Engagement fort, dafür zu sorgen, dass sich Organisationen, Mitarbeiter und Kunden in der sich schnell entwickelnden digitalen Welt sicher fühlen und stellen die Frage: Würden Sie einem Fremden die Schlüssel zu Ihrem Haus anvertrauen?

In einer Zeit, in der die Cyberkriminalität kontinuierlich und unaufhaltsam zunimmt, verhindert die Implementierung eines Zero-Trust-Ansatzes, dass Ihre Geräte und Lieferanten zu einem weiteren Angriffsziel für Hacker werden.

Wir erläutern die Auswirkungen, wenn Menschen ihre eigene Technologie für die Arbeit nutzen. Informieren Sie sich darüber, wie Ransomware-Angriffe (wieder) in die Höhe schnellen und Hacker sich besser tarnen. Und erfahren Sie, wie Hacker über Ihre Softwareanbieter an Ihre Daten gelangen können.

Die Cyberkriminalität entwickelt sich weiter und die Angriffsfläche ist größer als je zuvor. Die globale Cybercrime-Branche ist organisiert und nutzt alle Vorteile.

Ändern Sie Ihren Blickwinkel und betrachten Sie Ihre Mitarbeiter als erste Abwehrinstanz.

Nutzen Sie diesen Leitfaden, um die notwendigen Schritte einzuleiten und Ihr Unternehmen besser zu schützen."

Andrzej Kawalec
Head of Security Portfolio bei Vodafone Business

Einleitung

Die Zeiten, in denen Sie die volle Kontrolle darüber hatten, welche Technologien Ihre Mitarbeiter benutzen, gehören inzwischen der Vergangenheit an.

Heutzutage denkt man kaum noch darüber nach, welche Gefahren drohen, wenn private Endgeräte für die Arbeit genutzt werden oder mit einem Kollegen auf WhatsApp gechattet wird. Die Hacker freuen sich allerdings, wenn Sie keine Kontrolle mehr darüber haben. Aber wie können Sie Ihre Daten schützen, wenn Sie nicht wissen, welche Geräte, Software oder Cloud-Dienste Ihre Mitarbeiter verwenden?

In den letzten 18 Monaten sind die Grenzen zwischen Zuhause und Arbeit immer mehr verschwommen. Ihre Mitarbeiter haben an ihren eigenen Schreibtischen gesessen, haben ihren eigenen Kaffee getrunken und haben ihre eigene Technologie ausgewählt. Ihre Mitarbeiter greifen womöglich von ihren eigenen Computern, Tablets oder Telefonen auf Ihre Daten zu. Sie kommunizieren mit Ihren Kollegen über Chat-Apps wie WhatsApp, Slack und Zoom. Und sie teilen Dokumente über Dropbox und ungesicherte USB-Laufwerke.

Hier sind einige der Themen, auf die wir eingehen werden:

Shadow-IT: Davon sprechen wir, wenn Mitarbeiter ohne das Wissen des Unternehmens Geräte, Software und öffentliche Cloud-Dienste wie File-Sharing-Apps oder Video-Meetings nutzen.

BYOD – Bring Your Own Device: Das heißt, Sie erlauben Ihren Mitarbeitern, mit ihrer eigenen Technologie auf Ihr Netzwerk zuzugreifen. In diesen Fällen wissen Sie über das Gerät Bescheid und können die richtigen Sicherheitsrichtlinien einführen.

Hybrides Arbeiten: Davon sprechen wir, wenn Ihre Mitarbeiter sowohl im Büro als auch außerhalb arbeiten. Dadurch sehen wir immer mehr „Shadow-IT" und „Bring Your Own Device".

Ransomware: Hiervon sprechen wir, wenn Cyberkriminelle Ihre Daten stehlen oder Ihre Systeme auf andere Weise angreifen und ein Lösegeld verlangen, bevor Sie wieder den Zugang zu Ihren Systemen oder Daten erhalten.

Phishing: Das heißt, Hacker senden gefälschte E-Mails (Phishing), SMS (Smishing) oder gefälschte Absenderrufnummern (Vishing) oder leiten Sie auf gefälschte Websites, die aber seriös aussehen, weiter. Sie zielen alle darauf ab, Menschen dazu zu bringen, den Hackern Informationen oder Zugang zu Ihren Systemen zu geben.

Angriffe auf Ihre Lieferkette: Statt Ihr Unternehmen direkt anzugreifen, nutzen Hacker eine Schwachstelle in Ihrer Lieferkette aus. Sie greifen einen Ihrer Zulieferer an, um Störungen und Ausfälle zu verursachen oder um Daten zu stehlen und sich Zugang zu Ihren Systemen zu verschaffen. All das zielt darauf ab, Ihrer Firma zu schaden. Alternativ greifen sie über Sie eine andere Firma an. In jedem Fall kann Ihr Geschäft gestört werden, auch wenn der Angriff einem anderen gilt.

Einleitung

Die Zeiten, in denen Sie die volle Kontrolle darüber hatten, welche Technologien Ihre Mitarbeiter benutzen, gehören inzwischen der Vergangenheit an.

Die Pandemie hat Ihren Mitarbeitern die Entscheidungen über die Technologie überlassen

Es ist natürlich nichts Neues, dass Mitarbeiter selbst Ihre Entscheidungen über Technologien treffen. Der Trend hat aber stark zugenommen, als die Welt anfing, von zu Hause aus zu arbeiten. Bitglass, ein Unternehmen für Cybersicherheit, berichtet, dass 47 % der Unternehmen im Zuge der Umstellung auf Remote Work eine Zunahme der Nutzung privater Endgeräte für die Arbeit melden.[1]

Natürlich wird Remote Work auch nicht einfach verschwinden. Einige der weltweit führenden Unternehmen wie HSBC, KPMG und Deutsche Bank geben an, in Zukunft eine hybride Strategie verfolgen zu wollen.[2] Dabei werden die Mitarbeiter einen Teil ihrer Zeit im Büro und einen Teil außerhalb des Büros verbringen.

Mehr Konnektivität bedeutet mehr Risiken … und auch mehr Vorteile

In der Cybersicherheit sprechen wir von der „Angriffsfläche“ Ihres Unternehmens. Wenn alle Mitarbeiter im Büro an firmeneigenen Endgeräten und der entsprechenden Software arbeiten, ist die Angriffsfläche klein. Je mehr Geräte und Apps Sie verwenden und je mehr Mitarbeiter von außerhalb arbeiten, desto größer ist die Angriffsfläche. Und desto anfälliger sind sie für Angriffe. Das ist tatsächlich kein Problem – zumindest solange Sie die Geräte und die Software kennen, die auf Ihr Netzwerk zugreifen, und solange Sie die notwendigen Kontrollen und Verfahren haben, um sie zu sichern.

In diesem eBook gehen wir der Frage nach, wie es für Ihr Unternehmen sogar von Vorteil sein kann, wenn Ihre Mitarbeiter die Freiheit haben über Technologien zu entscheiden, die sie benutzen. Zusätzlich werfen wir einen Blick auf die aktuellen Bedrohungen, denen Sie sich bewusst sein sollten, auf die besten Methoden, Ihre Daten zu schützen und darauf, wie wir Ihnen helfen können.

Spotlight 1

Immer mehr Menschen benutzen ihre eigene Technologie für die Arbeit

Als Shadow-IT bezeichnen wir alle von Mitarbeitern genutzten Technologien. Seien es Geräte, Cloud-Dienste oder Apps, die Ihr Unternehmen nicht genehmigt hat. Sie bleiben unbemerkt und sind entsprechend ungeschützt. Anstatt ihren Mitarbeitern die Nutzung eigener Technologien zu untersagen, machen sich Unternehmen die Idee zu eigen – und bezeichnen es als BYOD bzw. Bring Your Own Device. Mit den richtigen Kontrollen und Richtlinien können Ihre Mitarbeiter die Tools nutzen, die ihnen gefallen, und werden dabei durch die Sicherheit des Unternehmens geschützt.

39%

Laut einem aktuellen Bericht von Trend Micro verwenden 39 % der Mitarbeiter regelmäßig private Geräte, um auf Unternehmensdaten zuzugreifen.

Hacker können eine größere Angriffsfläche als je zuvor nutzen

Wenn Ihre Mitarbeiter eine Aufgabe erledigen müssen und sie mit den Tools, die Sie zur Verfügung stellen, nicht gut umgehen können, werden sie welche finden, mit denen sie besser zurechtkommen. Ihnen ist sicher bekannt, dass Ihre Mitarbeiter gelegentlich ihre eigenen Geräte und eigene Software nutzen. Und wie viele Unternehmen sind Sie vielleicht nachlässig geworden, weil einfach „bisher noch nichts passiert ist“. Aber das ist so als hätten Sie keinen Feuermelder, weil es bei Ihnen noch nie gebrannt hat.

Laut einem aktuellen Bericht von Trend Micro nutzen 39 % aller Mitarbeiter regelmäßig eigene Geräte, um auf Unternehmensdaten zuzugreifen.[3] Diese Telefone, Tablets und Laptops werden häufig direkt mit den IT-Systemen ihrer Firmen verbunden, aber auch über Cloud-Dienste und -Apps. Noch besorgniserregender ist die Tatsache, dass mehr als ein Drittel der Mitarbeiter keine Passwörter auf all ihren privaten Geräten haben. Das ist eine ziemlich große Sicherheitslücke.

Und wenn ein Virus ein privates Gerät infiziert hat, kann es auf das Unternehmensnetzwerk übergreifen. In ähnlicher Weise gab mehr als die Hälfte der Mitarbeiter, die remote arbeiten, an, IoT-Geräte an ihr Heimnetzwerk angeschlossen zu haben – Geräte mit bekannten Schwachstellen. Sie können sehr einfach als Sprungbrett für Hacker dienen, um in Ihr Unternehmensnetzwerk einzudringen.

Spotlight 1

Immer mehr Menschen benutzen ihre eigene Technologie für die Arbeit

Ihren Mitarbeitern technologische Freiheit zu geben ist gut fürs Geschäft

Laut einer kürzlich durchgeführten Studie haben Unternehmen eine Vielzahl von Vorteilen festgestellt, wenn sie ihren Mitarbeitern erlauben, die eigenen Geräte mit eigener Software zu nutzen.[4] 68 % der Befragten berichteten, dass ihre Mitarbeiter produktiver seien, 53 % berichteten von größerer Zufriedenheit ihrer Mitarbeiter und 45 % von einer Kostenreduzierung.

Zu den weiteren Vorteilen gehören:

- größere Flexibilität für Mitarbeiter, wie und wo sie arbeiten.
- mehr Engagement, Produktivität und Effizienz unter Mitarbeitern.
- mehr Übereinstimmung zwischen dem Unternehmen und dem Verhalten der Mitarbeiter.
- größeres Vertrauen gegenüber der Unternehmensleitung.
- mehr Geräte, unter denen Mitarbeiter wählen können.
- geringere Kosten für Geräte für Ihr Unternehmen. (Möglicherweise werden Sie aber noch kommerzielle Softwarelizenzen bezahlen müssen.)[5]

Fallstudie

Ein einziges Passwort kann eine offene Tür sein

Im April 2021 haben sich Hacker Zugang zur größten Treibstoffpipeline der USA verschafft: der Colonial Pipeline.[6] Der Angriff führte zu Ölknappheit an der Ostküste der USA. Und das konnte alles wegen eines einzigen Passworts für einen einzigen veralteten Dienst geschehen.

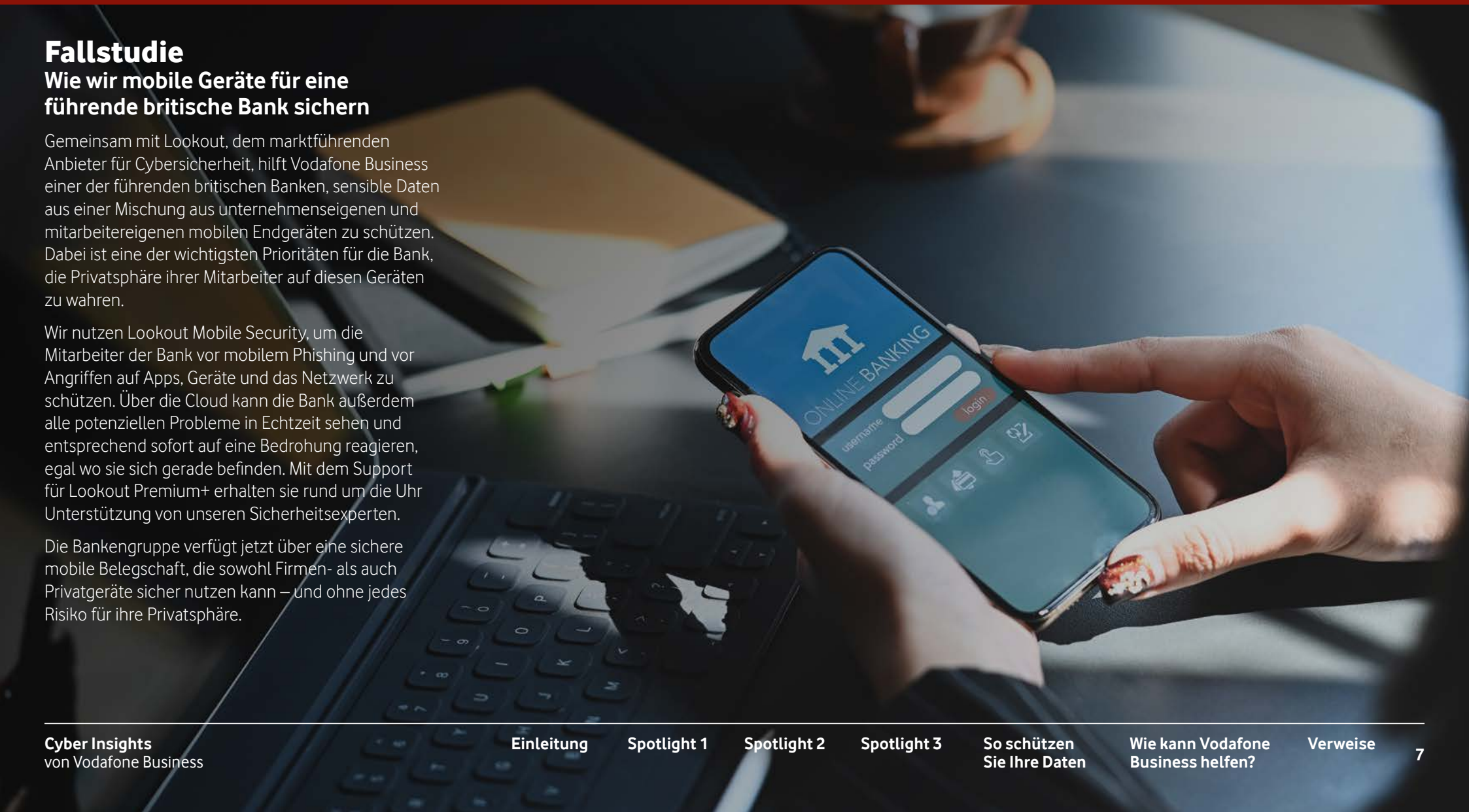
Der Angriff erfolgte über ein altes virtuelles privates Netzwerk, über das Mitarbeiter miteinander kommunizieren konnten. Das Konto wurde nicht einmal genutzt und die Software war veraltet. Die Hacker haben das Passwort über das Dark Web gefunden, vermutlich weil der Mitarbeiter dasselbe Passwort für mehrere Dienste verwendet hat.

Wie man sieht, kann ein einziges Passwort zu einem großen Angriff führen, wenn Sie Ihren Mitarbeitern erlauben, ihre eigenen Geräte mitzubringen. Es zeigt auch, weshalb Unternehmen grundsätzlich niemandem vertrauen sollten. (Mehr dazu später.) Das bedeutet aber nicht, dass Mitarbeiter ihre eigenen Geräte nicht verwenden können, sondern vielmehr dass Sie ihnen den Zugriff auf Ihr Netzwerk und Ihre Unternehmenssysteme nicht anvertrauen sollen. Erlauben Sie ihnen nur eingeschränkten Zugriff und fügen Sie weitere Sicherheitsebenen hinzu. Denn Ihre Mitarbeiter könnten veraltete Software mit Sicherheitslücken verwenden, ihr persönliches Gerät mit anderen Familienmitgliedern teilen oder sensible Daten herunterladen.

> **Persönliche Geräte für die Arbeit zu verwenden ist für viele jetzt die Norm, kann aber dazu führen, dass Sie das Gefühl haben, ein Doppelleben zu führen. Einerseits finden sie es bequem, ihr persönliches Smartphone oder Tablet für die Arbeit zu nutzen andererseits erlaubt es indirekt einen Zugriff auf persönliche Daten. Um die Vorteile von BYOD zu maximieren, ohne dabei die Risiken zu erhöhen, müssen Unternehmen und ihre Mitarbeiter ein Gleichgewicht zwischen der Wahrung der Privatsphäre der Mitarbeiter und der Kontrolle über die Unternehmensdaten auf den Geräten finden.**
>
> **Bharat Mistry, Technical Director (UK) bei Trend Micro**

Spotlight 1

Immer mehr Menschen benutzen ihre eigene Technologie für die Arbeit



Fallstudie

Wie wir mobile Geräte für eine führende britische Bank sichern

Gemeinsam mit Lookout, dem marktführenden Anbieter für Cybersicherheit, hilft Vodafone Business einer der führenden britischen Banken, sensible Daten aus einer Mischung aus unternehmenseigenen und mitarbeitereigenen mobilen Endgeräten zu schützen. Dabei ist eine der wichtigsten Prioritäten für die Bank, die Privatsphäre ihrer Mitarbeiter auf diesen Geräten zu wahren.

Wir nutzen Lookout Mobile Security, um die Mitarbeiter der Bank vor mobilem Phishing und vor Angriffen auf Apps, Geräte und das Netzwerk zu schützen. Über die Cloud kann die Bank außerdem alle potenziellen Probleme in Echtzeit sehen und entsprechend sofort auf eine Bedrohung reagieren, egal wo sie sich gerade befinden. Mit dem Support für Lookout Premium+ erhalten sie rund um die Uhr Unterstützung von unseren Sicherheitsexperten.

Die Bankengruppe verfügt jetzt über eine sichere mobile Belegschaft, die sowohl Firmen- als auch Privatgeräte sicher nutzen kann – und ohne jedes Risiko für ihre Privatsphäre.

Spotlight 2

Ransomware-Angriffe nehmen (wieder) stark zu und Hacker werden immer besser darin, unbemerkt zu bleiben

In unserem eBook vom letzten Quartal berichteten wir, von einem weltweiten Anstieg an Ransomware-Angriffen um 150 % im Jahr 2020. Erschreckend ist, dass im Jahr 2021 dieser Wert bereits in den ersten sechs Monaten übertroffen wurde. Bei diesen Angriffen dringen Cyberkriminelle in Ihr Netzwerk ein, um Daten zu stehlen, und sperren Sie aus Ihren Systemen aus oder übernehmen die Kontrolle. Sie müssen dann ein Lösegeld bezahlen, um Ihre Daten, den Zugriff, oder die Kontrolle wiederzuerlangen. Die einzige Alternative ist es, ein Backup Ihrer Systeme oder Daten wiederherzustellen, wobei der Hacker Ihre sensiblen Daten immer noch veröffentlichen kann.

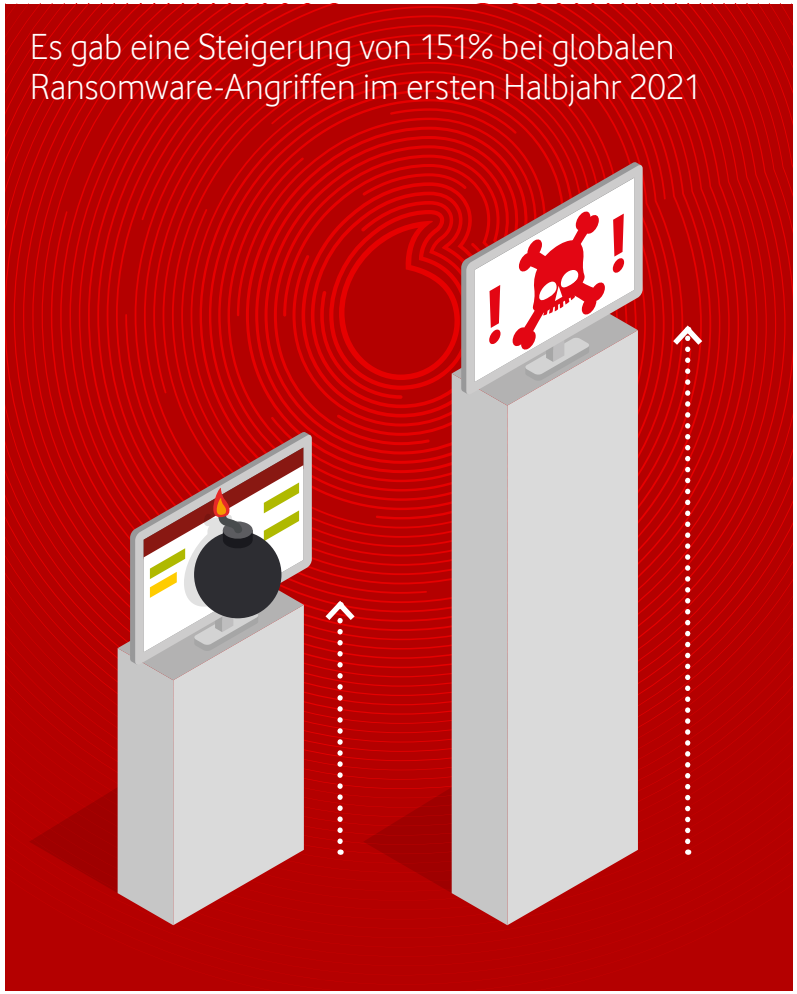
151%

Die weltweiten Ransomware-Angriffe haben um 151% zugenommen im ersten Halbjahr 2021.

Wenn Ihr Unternehmen Technologien verwendet, von denen Sie nichts wissen und die Sie nicht gesichert haben, ist es für Hacker viel leichter, Zugriff zu erhalten. Hacker verfolgen immer häufiger ein finanzielles Ziel und versuchen, ein Lösegeld zu fordern (und zu erhalten), bevor sie den Zugang wiederherstellen.

Laut Threatpost, einer Online-Publikation für Cybersicherheit, ist die Zahl der weltweiten Ransomware-Angriffe im ersten Halbjahr 2021 um 151 % gestiegen. Oder in konkreten Zahlen ausgedrückt: Zwischen Januar und Juni 2021 verzeichnete das Cybersicherheitsunternehmen SonicWall 304,7 Millionen Ransomware-Angriffsversuche. Im gesamten Jahr 2020 verzeichnete die Firma 304,6 Millionen Versuche. Mit 234 % ist Europa die Region mit dem größten Anstieg an Ransomware-Angriffen. Auf Länderebene liegen die Vereinigten Staaten mit einem Anstieg von 180 % vorne. Das Vereinigte Königreich lag mit einem Anstieg an Ransomware-Angriffen von 144 % an zweiter Stelle.

Threatpost berichtet darüber hinaus, dass laut FBI derzeit mehr als 150 verschiedene Arten von Ransomware weltweit im Umlauf seien – und diese Zahl steigt täglich.[7] Im Halbjahresbericht von Trend Micro zur Cybersicherheit heißt es, dass „im ersten Halbjahr von 2021 49 neue Ransomware-Familien aufgetaucht sind, was zeigt, dass Ransomware eine zunehmende Bedrohung darstellt.“ [8]



Spotlight 2

Ransomware-Angriffe nehmen (wieder) stark zu und Hacker werden immer besser darin, unbemerkt zu bleiben

Fallstudie

Geiselnahme einer Kaffeemaschine bei einem Ransomware-Angriff

Bei dieser Geschichte handelt es sich zwar nicht um einen herkömmlichen Angriff, sie zeigt aber, wie Hacker die Kontrolle über intelligente Geräte, also solche, die mit dem Internet verbunden sind, übernehmen können. Sie verdeutlicht auch das Risiko, dass Hacker intelligente Geräte nutzen, um sich Zugang zu Ihrem Netzwerk zu verschaffen. Solche Geräte sind u. a. intelligente Lautsprecher oder Uhren und sogar Waschmaschinen und Türklingelkameras, die Sie aus der Ferne über eine App bedienen können.

Forbes berichtete über einen Cybersicherheitsforscher beim Sicherheitsanbieter Avast, der es geschafft hat, eine intelligente Kaffeemaschine zu hacken.[9] Er fand dabei heraus, dass man über eine Android-App die Software der Kaffeemaschine aktualisiert. Und um diese Verbindung herzustellen, war die Kaffeemaschine WiFi-fähig. Darüber hinaus fand der Forscher heraus, dass diese Verbindung – und auch die Software-Updates selbst – unverschlüsselt und ungesichert waren.

Ursprünglich wollte der Forscher die Maschine in ein Gerät zum Schürfen von Kryptowährungen verwandeln, entschied aber letztendlich, dass es sich aufgrund der Geschwindigkeit des CPU nicht lohnen würde. Also übernahm er die Kontrolle über die Kaffeemaschine und ließ sie ständig piepen und Wasser kochen, sodass sie zu einem großen Ärgernis wurde. Die einzige Möglichkeit, daran etwas zu ändern, war es, ein Lösegeld zu zahlen … oder sie einfach auszustecken.

Im wirklichen Leben würde sich ein solcher Angriff zeitlich kaum für einen Hacker lohnen. Schließlich würde das zu erwartende Lösegeld nicht höher als die Kosten für den Austausch der infizierten Kaffeemaschine sein. Es zeigt aber, wie weit Sie denken müssen, wenn Sie überlegen, welche Geräte Zugang zu Ihrem Netzwerk haben könnten. Der Forscher bei Avast sagte, dass die Umkehrung des Hacks mit mehr Arbeit möglich sei. Dazu müsse die Kaffeemaschine so programmiert werden, dass sie über die WiFi-Verbindung den Router und andere Geräte angreife, die mit demselben Netzwerk verbunden seien. Sicher ist, dass Sie in Zukunft ganz anders über Kaffeemaschinen nachdenken werden.

Spotlight 2

Ransomware-Angriffe nehmen (wieder) stark zu und Hacker werden immer besser darin, unbemerkt zu bleiben

Fallstudie

Eine gefälschte Nachricht – auf einer vertrauenswürdigen Website – führt zu 40 Millionen Dollar Lösegeld

Kürzlich haben Hacker Phishing genutzt, um Ransomware in die Systeme eines großen US-amerikanischen Versicherungsunternehmens einzuschleusen. Berichten zufolge begann der Angriff mit einer gefälschten Nachricht auf dem Computer eines Mitarbeiters.[10] Darin hieß es, dass der Mitarbeiter seinen Internet-Browser (wie Internet Explorer, Chrome oder Firefox) auf die neueste Version aktualisieren müsse. Als der Mitarbeiter auf das gefälschte Update klickte, lud der Computer stattdessen eine Datei herunter, über die der Hacker in den Computer eindringen konnte.

Nur zwei Wochen nachdem der Angriff die Netzwerke lahmgelegt hatte, bezahlte die Versicherungsgesellschaft 40 Millionen Dollar für die Wiederherstellung ihrer Systeme.[11]

Bemerkenswert ist, dass diese gefälschte Nachricht erschien, als der Mitarbeiter sich auf einer seriös wirkenden Website befand – einer Seite, die er dachte, sorglos nutzen zu können. Wäre die Nachricht auf einer weniger vertrauenswürdigen Seite erschienen, hätte der Mitarbeiter sie womöglich nicht angeklickt. Hacker werden immer besser darin, Leute auszutricksen, und verstecken sich heutzutage an unerwarteten Orten, von denen aus sie angreifen können, wenn Leute weniger aufpassen.

Spotlight 3

Hacker gelangen über Ihre Zulieferer an Ihre Daten

Kein Unternehmen ist völlig unabhängig. Wir verlassen uns auf Partner, wie z. B. Software-Anbieter, die wiederum auf ihre Partner angewiesen sind – und so geht es immer weiter. Jeder vertraut seinem direkten Geschäftspartner.

Da Ihre Kunden auch wiederum Kunden haben, ist eine solche Lieferkette ein wahres Geschenk für Hacker. Indem sie ein Glied in der Kette angreifen, erreichen sie auch viele andere Firmen.

Was ist aber, wenn Sie nicht wissen, dass Sie Teil einer Lieferkette sind, weil Ihnen nicht bewusst ist, dass Ihre Mitarbeiter ein bestimmtes Gerät, eine bestimmte Software oder einen bestimmten Cloud-Dienst nutzen?

Zwar sind Ransomware und Phishing nach wie vor die größten Bedrohungen für Ihr Unternehmen, Kriminelle kombinieren diese Methoden aber zunehmend zu so genannten Lieferkettenangriffen. Auf diese Weise können Hacker viele Opfer erreichen, um potenziell viel Geld zu verlangen. Wenn sie z. B. einen Software-Anbieter angreifen, können sie Tausende seiner Kunden erpressen.

Diese Angriffe können an praktisch jedem Punkt der Kette beginnen und sich in jede Richtung ausdehnen. So können Kriminelle Ihr Unternehmen angreifen, um Zugang auf die Systeme Ihrer Zulieferer und Kunden zu erhalten. Sie sind also nicht nur durch die Verbindungen zu Ihren Zulieferern und Kunden gefährdet, sondern auch diese durch ihre Verbindung zu Ihnen. Wenn Sie wissen, welche Geräte, Software und Cloud-Dienste Ihre Mitarbeiter verwenden, können Sie Sicherheitsrichtlinien und -kontrollen einführen. Dadurch wird es für Hacker schwieriger, über einen Angriff auf Ihr Unternehmen Ihre Lieferkette anzugreifen bzw. Zugriff auf Ihre Systeme zu erhalten, indem sie zunächst eine andere Firma angreifen. Wenn Shadow-IT bei Ihnen verwendet wird und Sie nicht wissen, welche Technologien Zugriff auf Ihr Netzwerk und Ihre Daten haben – und Sie keine Sicherheitsvorkehrungen getroffen haben –, sind Ihre Systeme ein leichtes Ziel für Hacker.

Es ist nicht nur Ihre eigene Technologie, die Sie schützen sollten. Jedes Unternehmen, mit dem Sie zusammenarbeiten, muss Sicherheitsmaßnahmen ergreifen. Denken Sie daran, wie stark Ihre Netzwerke verknüpft sind: Sie tauschen Dateien aus oder besuchen sich sogar gegenseitig für persönliche Meetings. Vergewissern Sie sich, dass Sie alle neuen Zulieferer gründlich prüfen, bevor Sie einen Vertrag mit ihnen unterzeichnen, und richten Sie Verfahren ein, um regelmäßig Ihre Lieferkette zu überwachen. Verfügen sie über die richtigen Sicherheitsrichtlinien? Halten sie sich auch an diese?

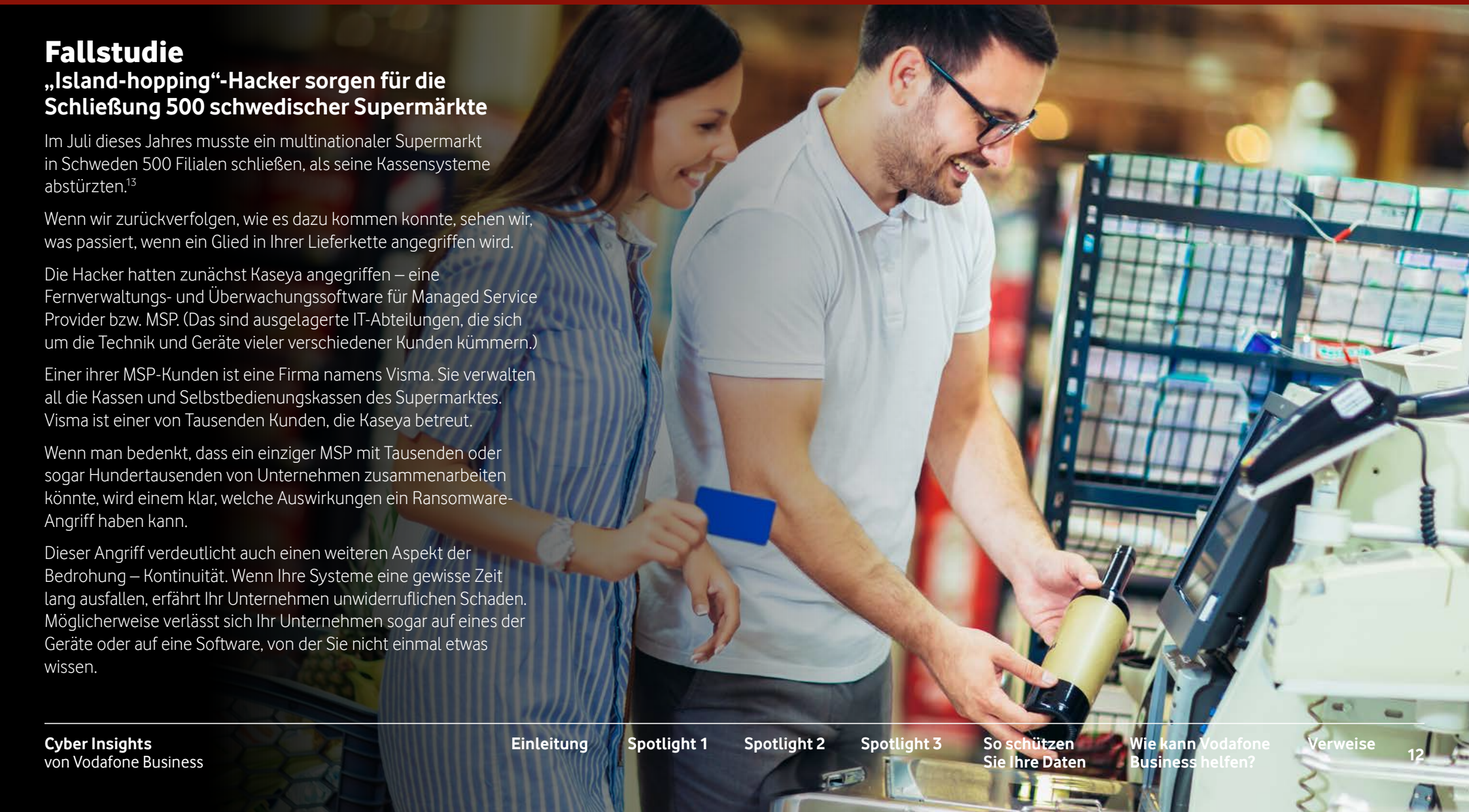
Kleinere Unternehmen neigen ggf. zu denken, dass sie für Hacker uninteressant sind. Dabei sind sie tatsächlich ein verlockendes Einfallstor, weil Kriminelle erwarten, dass sie weniger Sicherheitsvorkehrungen treffen.

Laut einem CNBC-Bericht zielen 43 % der Cyberangriffe auf kleine Unternehmen ab, von denen nur 14 % in der Lage sind, sich zu verteidigen.[12]

Hacker können jeden Punkt Ihrer Lieferkette angreifen

Spotlight 3

Hacker gelangen über Ihre Zulieferer an Ihre Daten



Fallstudie

„Island-hopping“-Hacker sorgen für die Schließung 500 schwedischer Supermärkte

Im Juli dieses Jahres musste ein multinationaler Supermarkt in Schweden 500 Filialen schließen, als seine Kassensysteme abstürzten.[13]

Wenn wir zurückverfolgen, wie es dazu kommen konnte, sehen wir, was passiert, wenn ein Glied in Ihrer Lieferkette angegriffen wird.

Die Hacker hatten zunächst Kaseya angegriffen – eine Fernverwaltungs- und Überwachungssoftware für Managed Service Provider bzw. MSP. (Das sind ausgelagerte IT-Abteilungen, die sich um die Technik und Geräte vieler verschiedener Kunden kümmern.)

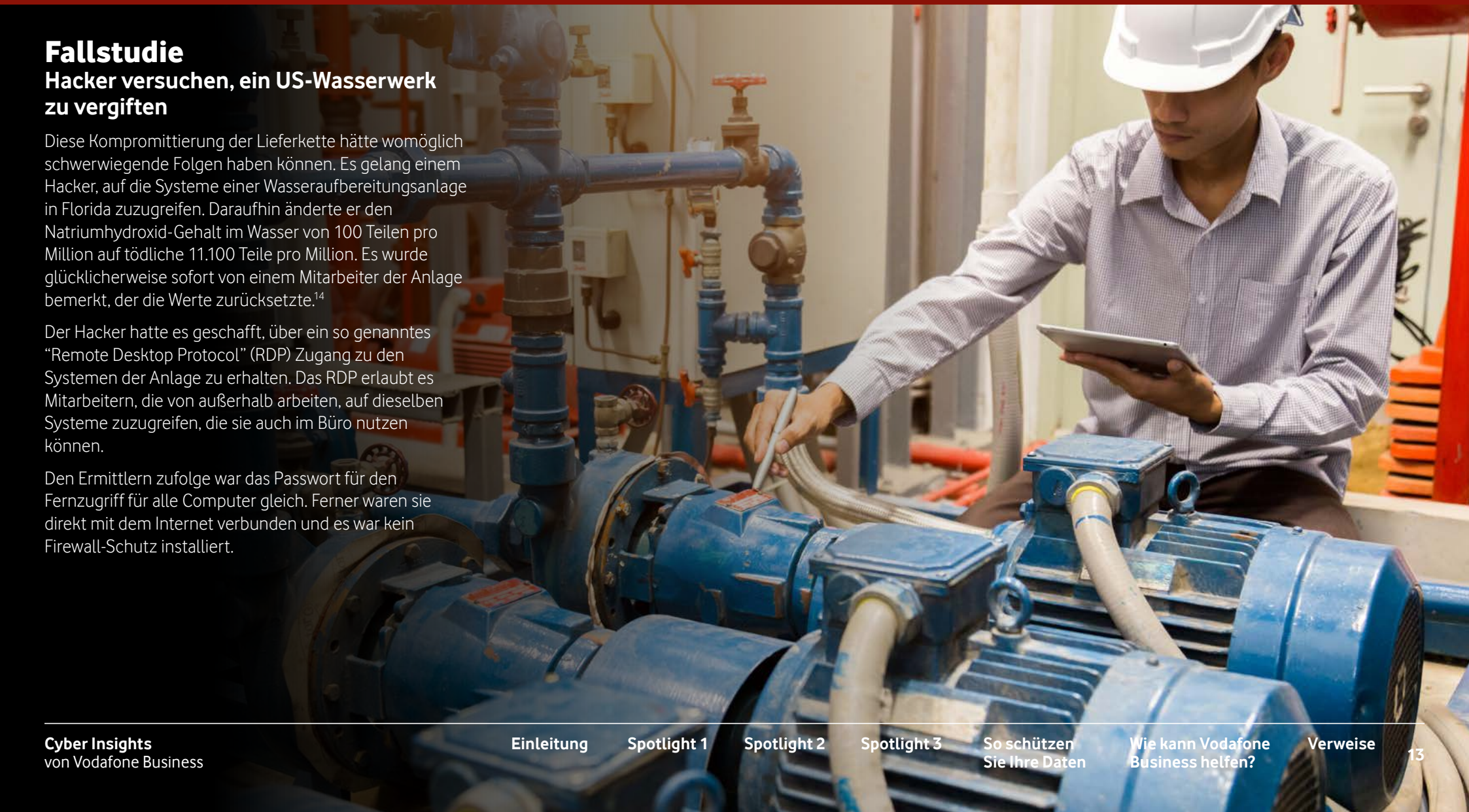
Einer ihrer MSP-Kunden ist eine Firma namens Visma. Sie verwalten all die Kassen und Selbstbedienungskassen des Supermarktes. Visma ist einer von Tausenden Kunden, die Kaseya betreut.

Wenn man bedenkt, dass ein einziger MSP mit Tausenden oder sogar Hundertausenden von Unternehmen zusammenarbeiten könnte, wird einem klar, welche Auswirkungen ein Ransomware-Angriff haben kann.

Dieser Angriff verdeutlicht auch einen weiteren Aspekt der Bedrohung – Kontinuität. Wenn Ihre Systeme eine gewisse Zeit lang ausfallen, erfährt Ihr Unternehmen unwiderruflichen Schaden. Möglicherweise verlässt sich Ihr Unternehmen sogar auf eines der Geräte oder auf eine Software, von der Sie nicht einmal etwas wissen.

Spotlight 3

Hacker gelangen über Ihre Zulieferer an Ihre Daten



Fallstudie

Hacker versuchen, ein US-Wasserwerk zu vergiften

Diese Kompromittierung der Lieferkette hätte womöglich schwerwiegende Folgen haben können. Es gelang einem Hacker, auf die Systeme einer Wasseraufbereitungsanlage in Florida zuzugreifen. Daraufhin änderte er den Natriumhydroxid-Gehalt im Wasser von 100 Teilen pro Million auf tödliche 11.100 Teile pro Million. Es wurde glücklicherweise sofort von einem Mitarbeiter der Anlage bemerkt, der die Werte zurücksetzte.[14]

Der Hacker hatte es geschafft, über ein so genanntes "Remote Desktop Protocol" (RDP) Zugang zu den Systemen der Anlage zu erhalten. Das RDP erlaubt es Mitarbeitern, die von außerhalb arbeiten, auf dieselben Systeme zuzugreifen, die sie auch im Büro nutzen können.

Den Ermittlern zufolge war das Passwort für den Fernzugriff für alle Computer gleich. Ferner waren sie direkt mit dem Internet verbunden und es war kein Firewall-Schutz installiert.

So schützen Sie Ihre Daten

Gehen Sie stets davon aus, dass Sie nichts und niemandem trauen können

Wenn Sie einer Schlange begegnen – und kein ausgesprochener Schlangenexperte sind –, gehen Sie am besten davon aus, dass die Schlange höchst gefährlich ist. Das gilt auch für jedes Gerät und jede Software, welche(s) auf Ihr Netzwerk oder Ihre Daten zugreifen möchte.

Beim Zero-Trust-Konzept geht man davon aus, nicht grundsätzlich jedem Gerät oder jeder Person im Netzwerk vertrauen zu können. Entsprechend muss stets die Identität aller Personen überprüft werden, die auf Ihre Netzwerk zugreifen wollen. Es bedeutet aber nicht, dass man seinen Mitarbeitern nicht vertrauen sollte. Ganz im Gegenteil: Es nimmt ihnen die Last ab, für die Sicherheit ihrer Daten und Werte zu sorgen. Mit dem Zero-Trust-Konzept können Sie Ihre Mitarbeiter dabei unterstützen, überall und auf jedem Gerät sicher zu arbeiten. Sie schützen sowohl Ihre Mitarbeiter als auch Ihr Unternehmen gegen Bedrohungen.

Ihre Sicherheits-Checkliste

Ob es sich um einen Ransomware-Angriff, Phishing oder einen Angriff auf die Lieferkette handelt – Sie können Ihre Daten vor Kriminellen schützen. Bedenken Sie, dass es bei der Sicherheit genauso auf die Menschen wie auf die Technologie, die sie verwenden, ankommt.

1 Finden Sie genau heraus, welche Geräte, Apps und Software Ihre Mitarbeiter nutzen.

- ✓ **Sprechen Sie im gesamten Betrieb mit Ihren Mitarbeitern**
  Fragen Sie die Mitarbeiter, was sie verwenden. Und fragen Sie sie vor allem, was sie brauchen. Wenn Sie Ihnen die Tools geben, die sie brauchen, ist es weniger wahrscheinlich, dass sie ihre eigenen suchen.
- ✓ **Seien Sie sich darüber im Klaren, welche Daten sich wo befinden**
  Fragen Sie Ihre Mitarbeiter, welche Art von Daten sie auf den Geräten speichern und teilen und welche Software sie dazu verwenden. Führen Sie eine Risikobewertung der Technologie durch, um sicherzustellen, dass Sie ihr vertrauen können.
- ✓ **Erstellen Sie ein Bestandsverzeichnis**
  Nutzen Sie das Active Directory von Microsoft, um Ihre IT in einer besser verwaltbaren Struktur zu organisieren.

2 Informieren Sie Ihre Mitarbeiter über die neuesten Bedrohungen und Sicherheitsempfehlungen

- ✓ **Stellen Sie sicher, dass Ihre Mitarbeiter Software-Updates installieren**
  Eine der einfachsten und wichtigsten Maßnahmen zum Schutz Ihrer Daten, die Sie ergreifen können, ist es, Software-Updates auf dem Laufenden zu halten. Mit Software-Updates werden alle bekannten Sicherheitslücken behoben.
- ✓ **Achten Sie auf gefälschte E-Mails, SMS, Anrufe und Websites**
  Kriminelle werden immer besser darin, sich zu tarnen. Sie senden E-Mails von scheinbar internen Adressen, erstellen realistisch aussehende Websites und rufen von Nummern aus an, die Smartphones als seriöse Unternehmen erkennen. Klären Sie Ihre Mitarbeiter darüber auf, auf was sie achten müssen und wie sie Verdächtiges erkennen.
- ✓ **Entwickeln Sie einen sicheren Umgang mit Passwörtern– für das gesamte Unternehmen**
  Klären Sie Ihre Teams über die besten Praktiken bei Passwörtern auf, z. B. dass sie keine Wörter aus dem Wörterbuch verwenden. Oder noch besser: Verwenden Sie einen Passwortmanager, der jedes Mal automatisch neue Passwörter generiert. Ein zentraler Passwortmanager kann Ihren Administratoren auch dabei helfen, herauszufinden, welche Software Ihre Mitarbeiter verwenden, ohne dabei ihre Anmeldedaten preiszugeben.

So schützen Sie Ihre Daten

Gehen Sie stets davon aus, dass Sie nichts und niemandem trauen können

Ihre Sicherheits-Checkliste

Ob es sich um einen Ransomware-Angriff, Phishing oder einen Angriff auf die Lieferkette handelt – Sie können Ihre Daten vor Kriminellen schützen. Bedenken Sie, dass es bei der Sicherheit genauso auf die Menschen wie auf die Technologie, die sie verwenden, ankommt.

3 Verwenden Sie die Multi-Faktor-Authentifizierung

✓ **Hierbei wird sichergestellt, dass eine Person zwei (oder mehr) hat von:**

- etwas, das sie kennen (wie ihr Passwort),
- etwas, das sie besitzen (wie ihr Handy),
- etwas, das sie sind (wie ihr Fingerabdruck).

Diese zusätzlichen Maßnahmen verringern das Risiko, da es sehr schwierig ist, an alle zu kommen oder sie zu fälschen.

4 Arbeiten Sie an einer positiven Kultur

✓ **Viele Menschen mögen Angst haben, über Technologien zu sprechen, die sie unerlaubt verwenden.**

Sie befürchten möglicherweise, dass Sie die Technologien verbieten oder dass sie Konsequenzen zu erwarten haben. Geben Sie Ihren Mitarbeitern die Möglichkeit, anzugeben, welche Software oder Dienste sie anonym verwenden, und versichern Sie ihnen, dass ihre tägliche Arbeit nicht dadurch beeinträchtigt wird.

5 Kontrollieren Sie Ihre Lieferkette

✓ **Sie sind berechtigt, Ihre Zulieferer zu überprüfen und Berichte über ihre Sicherheitsmaßnahmen zu fordern.**

Stellen Sie sicher, dass Sie – noch bevor ein Angriff erfolgt – von diesem Recht Gebrauch machen. Sie sollten Ihre gesamte Lieferkette kennen und wissen, ob Ihre Zulieferer wiederum eigene Subunternehmer nutzen. Legen Sie Mindestanforderungen und bewährte Praktiken fest und überprüfen Sie regelmäßig, ob die Firmen richtig mit den Risiken umgehen und Ihre Standards einhalten.

Wie kann Vodafone Business helfen?

Wir verstehen die Herausforderungen, die Sie zu bewältigen haben. Sprechen Sie also mit Ihrem Kundenbetreuer oder besuchen Sie unsere Website, um mehr über die Sicherheitslösungen zu erfahren, die für Sie richtig sind.

Stellen Sie mit Cyber Exposure Diagnostics Ihre Sicherheit auf den Prüfstand

In Zusammenarbeit mit Accenture können wir anhand realer Bedrohungsszenarien analysieren, wie widerstandsfähig Ihre Sicherheit ist. Anschließend erhalten Sie einen umfassenden Bericht, eine Liste von Maßnahmen und eine Roadmap mit Empfehlungen.

Schützen Sie alle mobilen Endgeräte mit Mobile Endpoint Security für kleine Unternehmen von Lookout

Seien Sie den Angreifern immer einen Schritt voraus mit Sicherheit auf Unternehmensniveau für Ihre mobilen Endgeräte. Sehen Sie mit Ihrem Online-Dashboard in Echtzeit, welchen mobilen Risiken Ihre Mitarbeiter ausgesetzt sind.

Schwachstellenanalyse von Vodafone Business

In Zusammenarbeit mit Accenture helfen wir Ihnen, ein besseres Verständnis für die Schwachstellen in Ihrem derzeitigen Geschäftssystem zu gewinnen. Wir identifizieren Schwachstellen, indem wir Ihre Infrastruktur von einer internen und externen Perspektive unter die Lupe nehmen.

Bewusstsein für Phishing

Durch unsere Partnerschaft mit Accenture können wir Sie darin beraten, wie Sie Ihr Unternehmen und Ihre Daten schützen können. So können Sie Ihre Mitarbeiter darüber aufklären, wie sie es vermeiden, einem Phishing-Versuch zum Opfer zu fallen.

Verweise

1. Study Finds Security Gaps Continue to be Pervasive across Bring Your Own Device (BYOD) Initiatives, Bitglass, 2021

2. HSBC, KPMG, and Deutsche Bank reveal 'hybrid' plan for workers return to Birmingham city centre offices, Birmingham Mail, 2021

3. Trend Micro Study Finds 39% of Employees Access Corporate Data on Personal Devices, 2020

4. BYOD Security report, Cybersecurities Insiders, 2021

5. How to Support BYOD in the Remote and Hybrid Workplace, CMSWire, 2021

6. Hackers Breached Colonial Pipeline Using Compromised Password, Bloomberg, 2021

7. Ransomware Volumes Hit Record Highs as 2021 Wears On, Threatpost, 2021

8. Midyear 2021 Cybersecurity Landscape Review: Attacks From All Angles Abound. Trend Micro, 2021

9. Coffee Machine Hit By Ransomware Attack—Yes, You Read That Right, Forbes, 2020

10. Beware of fake Windows 11 downloads, how an insurance giant was hacked, a ransomware gang attacked and more. IT Business, 2021

11. US insurance giant CNA Financial paid $40 million ransom to regain control of systems: report, 2021

12. Cyberattacks now cost companies $200,000 on average, putting many out of business, CNBC, 2019

13. Coop supermarket closes 500 stores after Kaseya ransomware attack, Bleeping Computer, 2021

14. Compromise of U.S. Water Treatment Facility, Cybersecurity & Infrastructure Security Agency, 2021

Together we can

vodafone business