Die Herausforderungen der Sicherheit mobiler Mitarbeiter – und wie man sie löst

#KingstonIsWithYou

Die Herausforderungen der Sicherheit mobiler Mitarbeiter – und wie man sie löst

Vorwort

Es ist an der Zeit, dass Ihre Mitarbeiter mehr als nur ein Lippenbekenntnis zur Datensicherheit ablegen. Sie wissen bereits, dass Remote-Arbeit einen Geschäftsmotor darstellt. Aber die Herausforderungen an die Netzwerksicherheit und die Einhaltung der DSGVO sind zu groß, um sie zu ignorieren. Viele Unternehmen halten es für eine unüberwindliche Herausforderung, ohne großen Aufwand die demonstrative Kontrolle über das IT-Ökosystem zu behalten. Aber dies muss nicht so sein. Kosten dürfen keine Entschuldigung sein.

Die Systeme, Dienstleistungen und Produkte sind vorhanden – und sie kosten weniger, als Sie vielleicht gedacht haben. Tatsächlich ist die Realität so, dass die Sicherheitsherausforderung nicht nur finanzieller oder technischer, sondern auch kultureller Natur ist. Sie können mit relativ geringem Aufwand die richtige IT-Umgebung für die Remote-Arbeit schaffen. Aber wenn Ihre Mitarbeiter nicht die richtige Einstellung und die geeigneten Verhaltensweisen in Bezug auf Sicherheit und Datenkonformität annehmen, wird Ihr Unternehmen in Schwierigkeiten geraten. Und die potenziellen Kosten von Verstößen sind unglaublich hoch.

Die Produkte sind bereits vorhanden. Aber Schulung ist alles.

Inhalt

Dieses kurze eBook wurde von drei Experten für Datensicherheit und Remote-Arbeit zusammengestellt.

Rob Allen
@Rob_A_kingston

Rob ist Direktor für Marketing und technische Dienste bei Kingston Technology und gehört dem Unternehmen seit 1996 an. In seiner Funktion ist Rob verantwortlich für die Bereiche PR, Soziale Medien, Channel-Marketing mit digitalen Marketingmedien und Kreatives für alle Kingston Marken und Produkte.

Rafael Bloom
@rafibloom73

Rafael ist der Direktor von Salvatore Ltd. In dieser Funktion unterstützt er Unternehmen bei der Bewältigung der strategischen, wirtschaftlichen und verfahrenstechnischen Herausforderungen und Chancen, die sich aus dem technologischen und regulatorischen Wandel ergeben.

Sarah Janes
@SarahkJanes

Sarah ist seit 2014 Geschäftsführerin der Layer 8 Ltd. Ihre Mission ist es, Sicherheitsmanager zu befähigen, einen effektiven Wandel der Cybersicherheitskultur in ganzen Organisationen, von kleinen Unternehmen bis hin zu großen Konzernen zu erreichen und aufrechtzuerhalten.

Die Herausforderungen der Sicherheit mobiler Mitarbeiter – und wie man sie löst

Inhaltsverzeichnis

Abschnitt 1 – Das Problem

Der Fernzugriff ist entscheidend

Die Zeiten, in denen ausschließlich an einem zentralen Bürostandort gearbeitet wurde, sind längst vorbei. Die Mitarbeiter greifen über ihr persönliches Smartphone auf Arbeits-E-Mails zu. Ihr COO verbringt Tage damit, von zu Hause oder in seinem Lieblingscafé zu arbeiten. Das Außendienstteam greift von den Standorten der Kunden auf geschäftskritische Geschäftsdaten zu. Fernarbeit ist die neue Norm.

Sie steigert die Produktivität und die Mitarbeiterbindung.[1] Sie reduziert die Geschäftskosten.[2] Sie ist gut für den Umweltschutz.[3] Untersuchungen zeigen, **dass 70% der Fachkräfte mindestens einmal pro Woche[4] aus der Ferne arbeiten**.

Eine Person alleine kann jedoch die Sicherheitsintegrität Ihrer gesamten Organisation gefährden, wenn sie die erforderlichen Sicherheitsprotokolle nicht einhält.

Die Einhaltung der DSGVO ist ein Muss

Angemessene Sicherheit darf nicht verhandelbar sein, sowohl für die Integrität Ihres Unternehmens als auch zur Vermeidung von Verstößen gegen die DSGVO-Konformität. Und die DSGVO ist ernst. Das ICO (Information Commissioner's Office) hat kürzlich Geldbußen an British Airways und die Hotelkette Marriott in Höhe von fast 300 Mio. Pfund wegen Datenschutzverletzungen verhängt.[5]

70% der Fachkräfte arbeiten mindestens einmal pro Woche aus der Ferne.[4]

Welche Art von Unternehmen sind gefährdet?

Wenn Ihre Mitarbeiter remote arbeiten oder mit eigenen Geräten auf Geschäftssysteme zugreifen, ist Ihr Unternehmen gefährdet. Das ist das Grundlegende.

[1] **Inc.com: Eine 2-jährige Stanford-Studie zeigt den erstaunlichen Produktivitätsschub der Arbeit von zu Hause aus -** www.inc.com/scott-mautz/a-2-year-stanford-study-shows-astonishing-productivity-boost-of-working-from-home.html

[2] **PGi: Was sind die Kosteneinsparungen durch Telearbeit? -** www.pgi.com/blog/2013/03/what-are-the-cost-savings-of-telecommuting/

[3] **FlexJobs: 5 Statistiken über die Umweltauswirkungen der Telearbeit -** www.flexjobs.com/blog/post/telecommuting-sustainability-how-telecommuting-is-a-green-job/

[4] **CNBC: 70% der Menschen weltweit arbeiten laut Studie mindestens einmal pro Woche aus der Ferne -** www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html

[5] **The Guardian: DSGVO-Bußgelder: Wo gehen die 300 Mio. Pfund von British Airways und Marriott hin? -** www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog

Abschnitt 2 – Die Herausforderungen des Fernzugriffs

Fernarbeit stellt mehrere Herausforderungen an die Sicherheit.

Sie können schwer zu vereinbaren sein, müssen aber für die Integrität Ihrer Organisation ernst genommen werden.

Sarah Janes
@SarahkJanes

Geschäftsführerin Layer 8 Ltd.

„Ein großes Anliegen im Rahmen der neuen DSGVO-Gesetzgebung ist es, dass ein Unternehmen die Kontrolle über die von ihm gespeicherten personenbezogenen Daten hat. Das ist nicht möglich, wenn sie nicht wissen, wo diese Daten gespeichert werden."

Unternehmen haben Mühe, ihre internen Systeme und Geräte mit dem Tempo auf dem neuesten Stand zu halten, in dem sich die Technologie im Allgemeinen entwickelt.

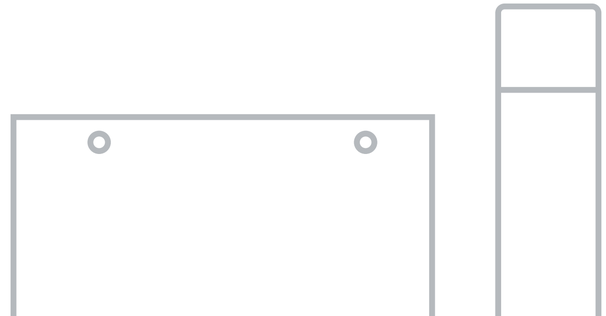
Tatsächlich sind 38% der von KMU eingestellten Remote-Mitarbeiter der Ansicht, dass sie nicht über die technologische Unterstützung oder das Fachwissen verfügen, das sie benötigen, wenn sie zu Hause oder in einem öffentlichen Raum arbeiten.

Dies kann dazu führen, dass Mitarbeiter Umgehungslösungen finden, die Ihre Datenschutzbemühungen verletzen und Ihr Unternehmen Sicherheitsbedrohungen aussetzen. Wenn Ihre Sicherheitsprotokolle nicht darauf ausgelegt sind, eine hohe Effizienz für Ihre Mitarbeiter zu bieten, werden sie Abhilfemaßnahmen finden, indem sie vertrauliche Informationen an Stellen wie Slack, Dropbox, persönlichen E-Mail-Konten oder auf privaten USB-Sticks speichern. Noch schlimmer ist, dass eine interne Feindschaft zwischen Ihrem IT-Sicherheitsteam und dem Rest Ihrer Mitarbeiter angestachelt wird. Ihr Unternehmen ist in Gefahr.

Rob Allen
@Rob_A_kingston

Direktor für Marketing und technische Dienste, Kingston Technology

„Meiner Erfahrung nach, ist es für die Mitarbeiter umso restriktiver und umständlicher, aus der Ferne zu arbeiten, je größer das Unternehmen ist – mit langen Anmeldezeiten und Sicherheitsmaßnahmen, die durchlaufen werden müssen."



Abschnitt 2 – Die Herausforderungen des Fernzugriffs

Bring-Your-Own-Device (BYOD)

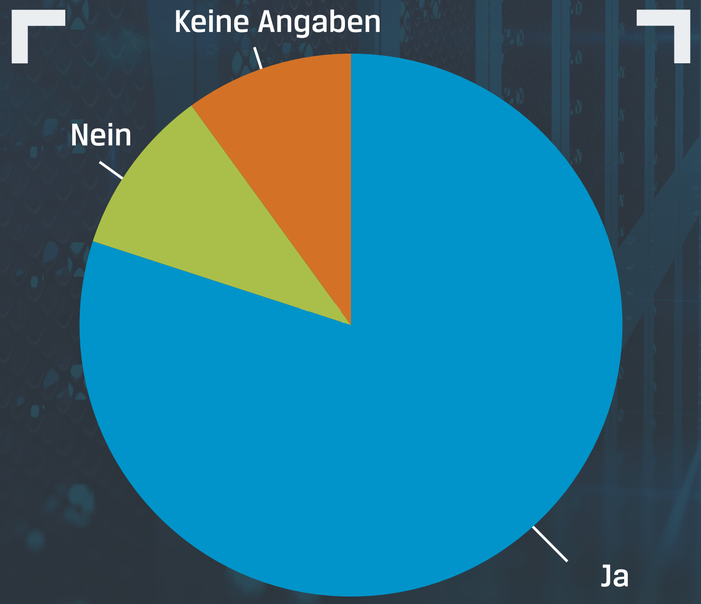
Es ist üblich, dass moderne Mitarbeiter ihre Smartphones zum Lesen von Arbeits-E-Mails verwenden, und von persönlichen Laptops und Tablets aus auf die Daten Ihres Unternehmens zugreifen. Das birgt Gefahren. Übertragen Ihre Mitarbeiter Daten aus dem Unternehmen? Ist ihre Hardware sicher vor Schäden und ihre Software geschützt? Das sind Fragen, die es zu beantworten gilt.

Sarah Janes
@SarahkJanes

Geschäftsführerin
Layer 8 Ltd.

„Unternehmen stehen vor einer massiven rückblickenden Herausforderung, nur um zu verstehen, wo ihre Daten gespeichert werden."

Haben Sie Bedenken, dass Mitarbeiter ungeeignete Umgehungslösungen für erzwungene Sicherheitsmaßnahmen finden?



Quelle: Kingston Survey 2019

Öffentliche WLAN-Netze

Es geht nicht nur darum, von zu Hause aus zu arbeiten. Was ist mit der Café-Crew, die sich mit dem Latte in der Hand einloggt? Öffentliche WLAN-Netzwerke sind ein Paradies für Hacker. Sie müssen Ihre Mitarbeiter mit den Werkzeugen ausstatten, um das Risiko zu minimieren.

Cyberangriffe und ausgeklügeltes Phishing

Phishing-E-Mails, die sich an einzelne Mitarbeiter richten, werden immer anspruchsvoller und überzeugender. Sind Ihre Mitarbeiter darin geschult, sie zu identifizieren? Was ist mit der sich ständig weiterentwickelnden Bedrohung durch Malware und Ransomware? Ihre Geräte – alle – müssen geschützt werden.

Abschnitt 3 – Die Infrastruktur des Fernzugriffs (und ein Hinweis zur sicherheitsbewussten Denkweise)

Die Technologie existiert, um die Sicherheitsherausforderungen der Remote-Arbeit zu vereinfachen. Sie muss außerdem kein Vermögen kosten.

Aufbau der richtigen Infrastruktur

Die Arbeitgeber müssen sicherstellen, dass ihre mobilen Mitarbeiter einfach und effizient auf die notwendigen Werkzeuge und Daten zugreifen können, um ihre täglichen Aufgaben zu erfüllen und produktiv arbeiten zu können. Es geht nicht unbedingt darum, neue Produkte hinzuzufügen, sondern die richtige Wahl zu treffen. Zum Beispiel werden die meisten Unternehmen Computer oder Laptops benötigen. Wählen Sie also verschlüsselte Festplatten oder SSDs. Auf diese Weise werden Unternehmensdaten bei Verlust oder Diebstahl vor dem Zugriff nicht autorisierter Personen geschützt. Darüber hinaus wird das ICO Sie im Falle eines Datenschutzverletzung positiver beurteilen, wenn Sie nachweislich Maßnahmen zum Schutz Ihrer Daten ergriffen haben.

Zusammenarbeit mit den richtigen Anbietern

Wenn es um IT-Sicherheit geht, gibt es unzählige Hersteller und Anbieter. Recherchieren Sie. Es geht darum, ein System einzurichten, das von einem vertrauenswürdigen Lösungsanbieter mit dem spezifischen Fachwissen für den Schutz Ihrer Mitarbeiter im mobilen Einsatz stammt.

VPNs

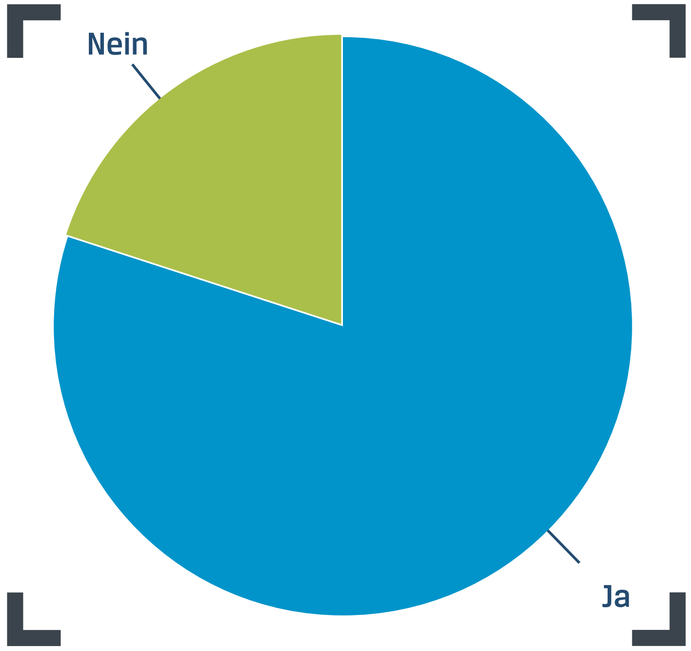
Wenn der Schutz Ihrer Organisation die Nutzung eines virtuellen privaten Netzwerks einschließt, dann werden die richtigen Werkzeuge in den Händen der richtigen Personen Ihre Risiken erheblich reduzieren. VPNs sind besonders geeignet für Mitarbeiter, die über öffentliche WLAN-Netze auf Geschäftsdaten zugreifen.

DLP-Software

Fast alle DLP-Software-Suiten bieten die Möglichkeit, den Zugriff auf Ihr Netzwerk einzuschränken, während bestimmte Geräte wie verschlüsselte USB-Sticks, die von Grund auf so konzipiert wurden, dass sie eindeutig identifizierbar sind, auf eine Whitelist gesetzt werden. Dies ist mit minimalen Kosten verbunden. (Werfen Sie einen Blick auf Kingstons USB-Angebot, das an Ihre Organisation angepasst werden kann.)

Mussten Sie wesentliche Änderungen vornehmen, um sicherzustellen, dass Ihr Unternehmen DSGVO-konform ist?

Quelle: Kingston Survey 2019



Abschnitt 3 – Die Infrastruktur des Fernzugriffs (und ein Hinweis zur sicherheitsbewussten Denkweise)

USB-Sticks und SSDs

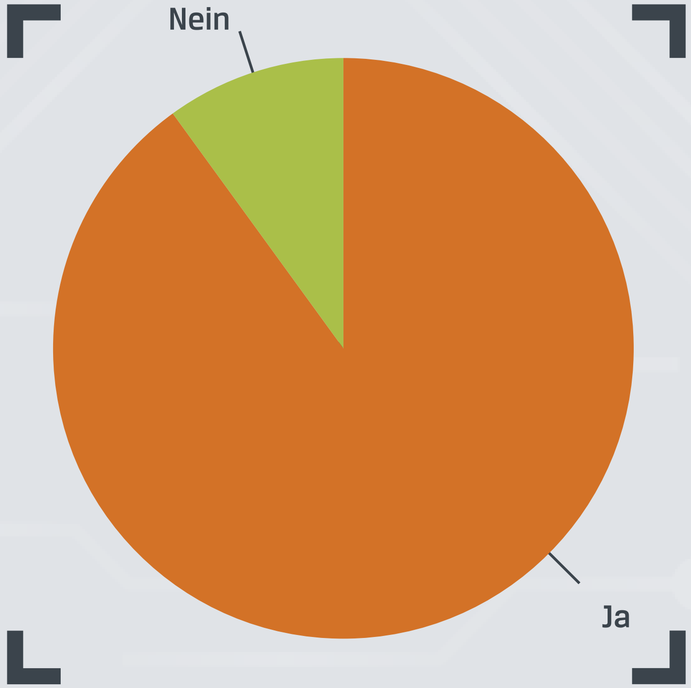
Die Bereitstellung verschlüsselter USB-Sticks und die Ausstattung der Notebooks Ihres Unternehmens mit hardwareverschlüsselten SSDs ist ein langer, langer Weg, um die Herausforderungen der Remote-Arbeit zu bewältigen. Mit einem verschlüsselten USB-Stick plus hardwareverschlüsselter SSD (WLAN oder nicht) sind Ihre Daten geschützt sowie jederzeit und überall verfügbar. Falls ein Gerät verloren geht oder gestohlen wird, können Sie sicher sein, dass niemand Zugriff auf die verschlüsselten Dateien hat. Sie können sogar verlorene USB-Sticks aus der Ferne zerstören.

Immer vom Schlimmsten ausgehen

Manchmal ist eine optimistische Denkweise nur die Verschleierung von blindem Glauben. Als Sicherheitsteam ist es immer das Beste – und sogar notwendig, vom Schlimmsten auszugehen. Vertrauen Sie auf Ihre Mitarbeiter und Ihre Sicherheitsmaßnahmen. Aber denken Sie immer an Worst-Case-Szenarien. Sie werden Wunder für die Integrität Ihrer Netzwerksicherheit bewirken, indem Sie davon ausgehen, dass sie verletzt werden kann – und wird.

Weiten Sie die Sicherheit durch Endgeräte-Sicherheitssoftware auch auf mobile Geräte am Arbeitsplatz aus? Beispielsweise USB-Sticks, Notebooks usw.

Quelle: Kingston Survey 2019



Abschnitt 4 – Die Schulung Ihrer Mitarbeiter ist der einzige Weg

Die richtige Technologie ist nur die halbe Miete. Die eigentliche Herausforderung besteht darin, was Ihre Mitarbeiter tun, wenn niemand hinsieht. Deshalb ist die Sicherheitsherausforderung ebenso eine Frage der Arbeitskultur wie eine Frage der Technologie. Ohne eine angemessene Schulung werden Ihre Mitarbeiter Dinge wie DSGVO, PECR und andere 'Regeln' immer maximal als notwendiges Übel betrachten.

Hier sind einige Tipps.

Keine Regeln ohne Grund

„Geh nicht hinter den Baum."
„Geh nicht hinter den Baum, weil dort ein Löwe ist."

Welcher Satz wird mehr beachtet werden? Menschen reagieren nicht ohne guten Grund auf Regeln. Helfen Sie Ihren Mitarbeitern zu verstehen, warum es überhaupt Regeln gibt.

Machen Sie es zu einer persönlichen Aufgabe für jeden

Ihre Mitarbeiter werden die Sicherheitsherausforderung besser verstehen, wenn Sie sie für ihr Leben relevant machen. Nehmen wir zum Beispiel die DSGVO. Um Ihrem Team zu helfen, zu verstehen, dass hinter jedem Datensatz eine Person steckt, lassen Sie sie darüber nachdenken, wie sie sich fühlen würden, wenn eine Organisation einen schlampigen Umgang mit ihren eigenen persönlichen Daten an den Tag legen würde. Wie würden sie sich fühlen, wenn ihre Details in die falschen Hände geraten würden?

„Wenn man einem Mitarbeiter erklärt, wie wichtig Sicherheit und die DSGVO für seine eigenen Interessen außerhalb des Arbeitslebens sind, beginnt er zu verstehen, warum eine Organisation verpflichtet ist, ihre Daten zu schützen."

Rafael Bloom
@rafibloom73
Direktor bei Salvatore Ltd.

„Letztendlich ist die beste Methode, um das Sicherheitsbewusstsein zu erhöhen, Gespräche mit den Mitarbeitern zu führen, um Strategien zu finden, die sowohl sicher als auch produktiv sind."

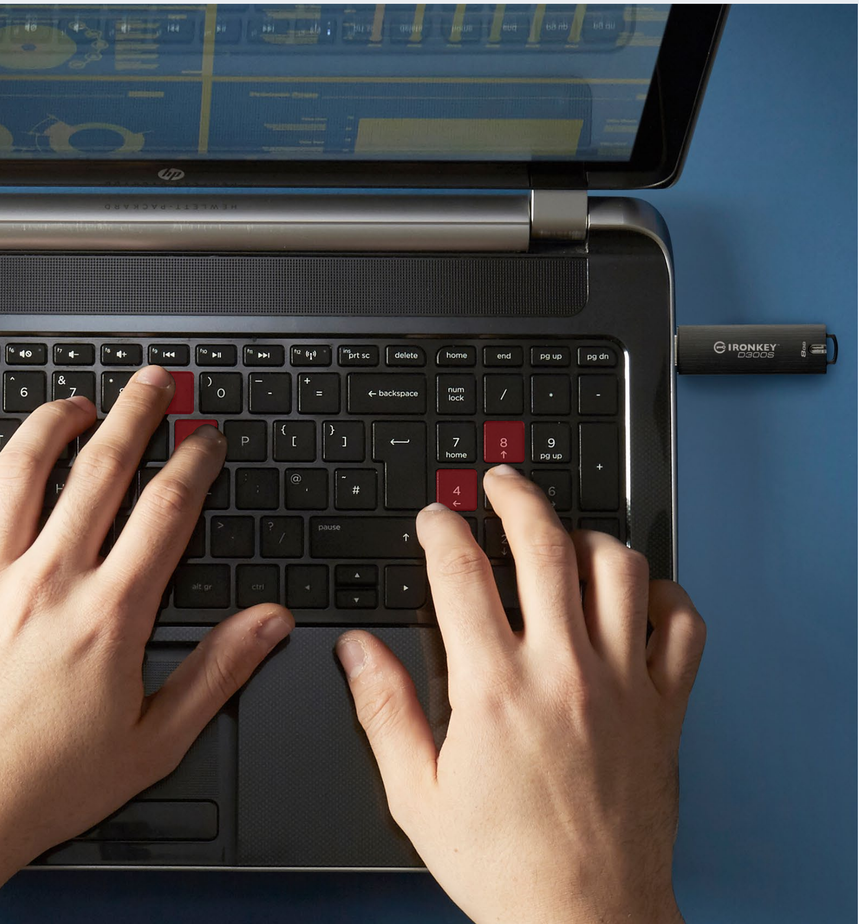
Sarah Janes
@SarahkJanes
Geschäftsführerin Layer 8 Ltd.

Quelle: Kingston Survey 2019

Überprüfen Sie regelmäßig die Nutzung externer Speicher Ihrer Mitarbeiter?

71%	11%	9%	9%
Ja	Nein	Nicht sicher	Keine Angaben

Abschnitt 4 – Die Schulung Ihrer Mitarbeiter ist der einzige Weg



Schulung steht am Anfang, nicht am Ende

Da die meisten Unternehmen intern einen Mangel an Sicherheitsschulungen anbieten, haben Unternehmen es übernommen, diese Lücke zu schließen. Aber hütet euch vor falschen Propheten. Die Schulung durch externe Berater ist oft in Richtung der Compliance-Anforderungen dieses Unternehmens (weil sie dafür Mittel erhalten können) verzerrt, was bedeutet, dass Ihre Mitarbeiter kein vollständiges Verständnis und Wertschätzung für Cybersicherheit entwickeln werden. Unsicheres Verhalten wird deshalb weiter fortbestehen.

Sarah Janes
@SarahkJanes

Geschäftsführerin
Layer 8 Ltd.

„Wenn Unternehmen ihr Verhalten wirklich ändern wollen, müssen sie mutig genug sein, um sich von Sicherheitsschulungen mit Multiple-Choice-Fragen zu lösen. Sie müssen darüber nachdenken, eine Schulung anzubieten, die die Grundlagen des Verständnisses für Sicherheit und Internet im Allgemeinen vermittelt."

Ebenso darf Schulung nicht nur als Feigenblatt dienen. Es fällt allzu leicht, zu glauben, dass Ihre Mitarbeiter, da sie geschult wurden, automatisch sichere Verhaltensweisen übernehmen und die gesetzlichen Regelungen einhalten. Das wäre eine gefährliche Naivität. Erfolg erfordert eine kontinuierliche Verhaltens- und Kulturpflege.

Rafael Bloom
@rafibloom73

Direktor bei
Salvatore Ltd.

„Ich habe „zertifizierte" Unternehmen erlebt, die Tabellen oder Notizbücher mit Passwörtern führen oder unverschlüsselte Kopien ihrer Festplatten über Nacht in den Autos der Mitarbeiter aufbewahren. Was nützt die Zertifizierung, wenn die Menschen die Grundlagen nicht verstehen?"

Verantwortung für den Datenschutz der Basis zuweisen

Eine Strategie, um den notwendigen kulturellen Wandel in Ihrem Unternehmen voranzutreiben, ist die Einführung von Sicherheitsverantwortliche, die Sicherheitsherausforderungen diskutieren und Sicherheitsprotokolle an Ihre Mitarbeiter vor Ort weiterreichen.

Sarah Janes
@SarahkJanes

Geschäftsführerin
Layer 8 Ltd.

„Diese Verantwortlichen führen Gespräche, um die Sicherheit für die Arbeitswelt jedes Mitarbeiters relevanter zu machen – in Verbindung mit Online-Schulungsmaterialien, die verwendet werden können, um die Veränderungen zu erleichtern – ist die beste Methode, um die Akzeptanz von sicheren Verhaltensweisen zu erreichen."

Zusammenfassung

Datenschutz und Cybersicherheit können sich wie eine lästige Verantwortung anfühlen. Die richtigen Tools machen die Fernarbeit jedoch einfach und sicher – und sie sind kostengünstig zu implementieren. Aber denken Sie daran, dass es einen kulturellen Wandel in Ihrer Organisation sowie die richtige Sicherheitsinfrastruktur geben muss, wenn sichere Verhaltensweisen von Ihren Mitarbeitern übernommen werden sollen.

Hier folgt eine kurze Zusammenfassung.

- Remote-Arbeit wird es weiter geben und hat viele Vorteile – darunter Produktivität, Mitarbeiterbindung und reduzierte Gemeinkosten. Die Remote-Arbeit bringt jedoch auch eine Reihe von Sicherheitsherausforderungen mit sich.
- Datenschutzverletzungen sind ein ernsthaftes Problem, da die ICO hohe Geldbußen verhängt, wenn die DSGVO missachtet wird.
- Nebenbei sind unsichere Hardware, Softwaremissbrauch und öffentliche WLAN-Netzwerke häufige Sicherheitsrisiken.
- Eine erfolgreiche Sicherheitsinfrastruktur muss ein effizientes Arbeiten für Ihre Mitarbeiter ermöglichen – und darf es nicht behindern. Andernfalls werden die Mitarbeiter sich Abkürzungen suchen und Abhilfemaßnahmen einsetzen.
- IT-Hersteller und -Anbieter aus der Forschung wählen diejenigen mit nachgewiesener Erfolgsbilanz aus.
- Tools wie verschlüsselte SSDs und USB-Sticks, VPNs und DLP-Software sind einfach zu implementieren und müssen nicht teuer sein.
- Erfolg bei Datenschutz und Sicherheit erfordert einen kulturellen und verhaltensbedingten Wandel in Ihrem Unternehmen. Ihre Mitarbeiter müssen verstehen, warum es die Regeln gibt, anstatt angewiesen zu werden, die Protokolle blind zu befolgen.
- Externe Berater können bei der Schulung der Mitarbeitersicherheit helfen – aber stellen Sie sicher, dass die Materialien geeignet sind und denken Sie daran, dass die Mitarbeiter nicht automatisch das richtige Verhalten übernehmen, nur weil sie in einer Schulung dazu aufgefordert wurden.
- Setzen Sie Sicherheitsverantwortliche ein, um Sicherheitsherausforderungen zu diskutieren und gutes Sicherheitsverhalten an der Basis zu steuern.

Über Kingston

Mit 32 Jahren Erfahrung verfügt Kingston über das Wissen, um Ihre Herausforderungen bei der Remote-Arbeit zu identifizieren und zu lösen – so können Ihre Mitarbeiter von überall sicher arbeiten, ohne Ihr Unternehmen zu gefährden.

#KingstonIsWithYou