Dell Umfrage unter Endbenutzern zum Thema Sicherheit

2017

Inhaltsverzeichnis

Einleitung

Wenn die nicht autorisierte Freigabe vertraulicher Daten Schlagzeilen macht, hängt dies in der Regel mit einem Skandal zusammen. Beispiele sind WikiLeaks, das Berichte eines anonymen Whistleblowers veröffentlicht, oder Unternehmen, die einen Wettbewerber wegen der Verwendung von Geschäftsgeheimnissen verklagen, die ein ehemaliger Mitarbeiter gestohlen hat.
Daten werden jedoch jeden Tag weltweit unter weitaus banaleren Umständen.
in Unternehmen freigegeben.

In den meisten Fällen hat dies keine Folgen für die Mitarbeiter, die diese Daten freigeben, da die Sicherheitsteams möglicherweise noch nicht einmal wissen, dass Protokolle verletzt wurden, und es auch keine nachteiligen Folgen für das Unternehmen hat.
Dieses Fehlen unmittelbarer Konsequenzen macht es Mitarbeitern allzu leicht, die Risiken zu verdrängen und die Sicherheitsprotokolle weiter zu verletzen. Irgendwann landet jedoch eine Datei in den falschen Händen und das Unternehmen findet sich im Zentrum einer verheerenden Situation, die katastrophale Auswirkungen auf die Finanzen oder den Ruf des Unternehmens haben kann.

Um herauszufinden, wie verbreitet die nicht sichere Freigabe vertraulicher Daten mittlerweile ist, hat Dell eine weltweite Umfrage unter 2.608 Mitarbeitern in Auftrag gegeben, die in Unternehmen mit mindestens 250 Mitarbeitern vertrauliche Daten verarbeiten. Die Ergebnisse zeigen, dass erstaunliche 72 Prozent der Mitarbeiter bereit sind, sensible, vertrauliche oder regulierte Unternehmensinformationen weiterzugeben.

72 %
der Mitarbeiter sind bereit, sensible, vertrauliche oder regulierte Unternehmensinformationen

In den meisten Fällen haben sie keine bösartigen Absichten. Sie versuchen einfach, so effizient und effektiv wie möglich ihre Arbeit zu tun. Es gibt zahlreiche legitime geschäftliche Gründe für die Weitergabe vertraulicher Informationen. Die in diesem Bericht vorgestellten Umfrageergebnisse zeigen jedoch, dass vielen Unternehmen nach wie vor die nötigen Verfahren fehlen, um sicherzustellen, dass diese Datenfreigabe auf sichere Weise erfolgt. Die Ergebnisse zeigen auch, dass sogar Mitarbeiter, die Informationen zu den Risiken erhalten haben, die mit einer Freigabe vertraulicher Daten
ohne Einhaltung von Sicherheitsprotokollen verbunden sind, die Konsequenzen
dieses Verhaltens nicht wirklich verstehen und einsehen. Sie wissen, dass ihre Handlungen risikobehaftet sind, lassen sich jedoch von den möglichen Konsequenzen nicht abschrecken. Diese Konsequenzen erscheinen ihnen im Vergleich zu den fassbaren Aufgaben, die sie jeden Tag erledigen müssen, fern und unwirklich.

Die Dell Umfrage unter Endbenutzern zum Thema Sicherheitzeichnet das Bild einer Mitarbeiterschaft, die zwischen zwei Erwartungen gefangen ist: Produktivität und Effizienz bei der Arbeit und Wahrung der Sicherheit der Unternehmensdaten. Um die Reibung zwischen diesen beiden konkurrierenden Zielen zu reduzieren, müssen Unternehmen ihren Mitarbeitern Informationen bereitstellen und Richtlinien und Verfahren durchsetzen, die die Sicherheit der Daten unabhängig davon gewährleisten, wo sich ihre Mitarbeiter befinden, ohne die Produktivität zu beeinträchtigen.

Wir hoffen, dass diese Ergebnisse nicht nur für Sicherheits- und IT-Experten nützlich sind, sondern auch für Geschäftsmanager, die Verantwortung für den Schutz von Daten und die Produktivität des Unternehmens haben.

Mitarbeiter geben vertrauliche Informationen wahrscheinlich weiter

Aus der Sicht der Mitarbeiter gibt es eine große Grauzone, wenn es um die Frage geht, wann die Freigabe von Daten autorisiert ist. Die meisten Mitarbeiter wissen wahrscheinlich, dass sie die Kreditkartendaten von Kunden unter keinen Umständen per E-Mail versenden dürfen. Aber ist es akzeptabel, eine vertrauliche Roadmap für einen Lieferanten freizugeben, wenn ein Vorgesetzter dies anordnet? Wie sieht es mit der Freigabe einer Übersicht zu einem noch nicht veröffentlichten Produkt für die Texter des Marketingteams aus, damit sie Texte für das Web vorbereiten können? Wie die Dell Umfrage unter Endbenutzern zum Thema Sicherheit zeigt, gibt es eine Reihe von Umständen, in denen es sinnvoll ist, vertrauliche Informationen freizugeben, um geschäftliche Initiativen zu unterstützen.

Beinahe drei von vier (72 Prozent) Mitarbeitern geben an, dass sie in bestimmten Umständen sensible, vertrauliche oder regulierte Unternehmensinformationen freigeben würden. Zu den am meisten genannten Umständen gehören: Anweisungen des Managements (43 Prozent); Freigabe für Personen, die spezifisch zum Empfang dieser Informationen autorisiert sind (37 Prozent); die Entscheidung, dass das Risiko für das Unternehmen sehr gering und der mögliche Nutzen sehr groß sind (23 Prozent); die Ansicht, dass ihnen dies helfen wird, ihre Arbeit effektiver zu erledigen (22 Prozent);
und die Ansicht, dass dies den jeweiligen Empfängern helfen wird, ihre Arbeit effektiver zu erledigen (13 Prozent).

72 %

der Mitarbeiter geben an, dass sie in bestimmten Umständen sensible, vertrauliche
oder regulierte Unternehmensinformationen freigeben würden.

Anweisungen des Managements

Die Informationen werden für Personen freigegeben, die

Das Risiko ist sehr gering und der Nutzen ist groß.

Es wird ihnen helfen, ihre Arbeit effektiver zu erledigen.

Es wird den jeweiligen Empfängern helfen, ihre Arbeit effektiver

In vielen Situationen, in denen Mitarbeiter nach persönlichem Ermessen eine Entscheidung darüber treffen, ob sie vertrauliche Daten freigeben sollen oder nicht, handeln sie unabhängig. Damit sind die betreffenden Mitarbeiter dafür verantwortlich, Risiko und Nutzen in Bezug auf die Freigabe bestimmter Arten von Informationen korrekt einzuschätzen.

Das ist einer der Gründe, warum sich Cyberkriminelle häufig als zuverlässige Partner, Mitarbeiter oder Unternehmen ausgeben, um Mitarbeiter dazu zu bringen, sensible Daten freizugeben. Mehr als einer von drei Mitarbeitern (36 Prozent) öffnet bei der Arbeit häufig E-Mails von unbekannten Absendern und ermöglicht damit möglicherweise Phishing-Angriffe, bei denen Cyberkriminelle versuchen, nicht autorisierten Zugriff auf sensible Informationen einer bestimmten Organisation oder Person zu erhalten, indem sie sich als zuverlässige Quelle ausgeben. Wenn Sicherheit zu einer Frage des persönlichen Ermessens wird, die fallbasiert von Hunderten oder sogar Tausenden von Mitarbeitern entschieden wird, verliert sie an Konsistenz und Wirkungskraft.

In bestimmten Branchen gehen Unternehmen mit Informationen um, die leichter als hoch sensibel kategorisiert werden können. Dennoch sind Mitarbeiter hier bereit, in bestimmten Umständen sensible Daten freizugeben. Beinahe vier von fünf Mitarbeitern in der Finanzdienstleistung (81 Prozent) sind bereit, sensible, vertrauliche oder regulierte Unternehmensinformationen freizugeben. Das bedeutet, dass in den vier größten Banken der Vereinigten Staaten mehr als 586.000 Mitarbeiter dazu tendieren, sensible Daten freizugeben.[i] Mitarbeiter im Bildungswesen (75 Prozent), im Gesundheitswesen (68 Prozent) und in Bundesbehörden (68 Prozent) sind zwar in geringerem Maß als Mitarbeiter in der Finanzdienstleistung zur Freigabe von Daten bereit, geben jedoch gelegentlich ebenfalls vertrauliche oder regulierte Daten frei.

Um sensible Unternehmensinformationen zu schützen, besteht die primäre Aufgabe eines Unternehmens darin, die Umstände, in denen Informationen freigegeben werden können, und die zulässigen Empfänger zu definieren. Dabei sollten so viele Szenarien wie möglich abgedeckt werden, um Mitarbeitern die nötigen Anleitungen bereitzustellen, damit sie im beruflichen Alltag Entscheidungen in Bezug auf Sicherheit treffen können. Es sollte jedoch auch darauf hingewiesen werden, dass die Freigabe der Daten selbst ebenfalls auf sichere Weise erfolgen sollte.

Der nächste Satz von Umfrageergebnissen zeigt, dass die wirkliche Gefahr möglicherweise gar nicht in der Art der freigegebenen Informationen liegt, sondern in der Art, wie diese Informationen freigegeben werden.

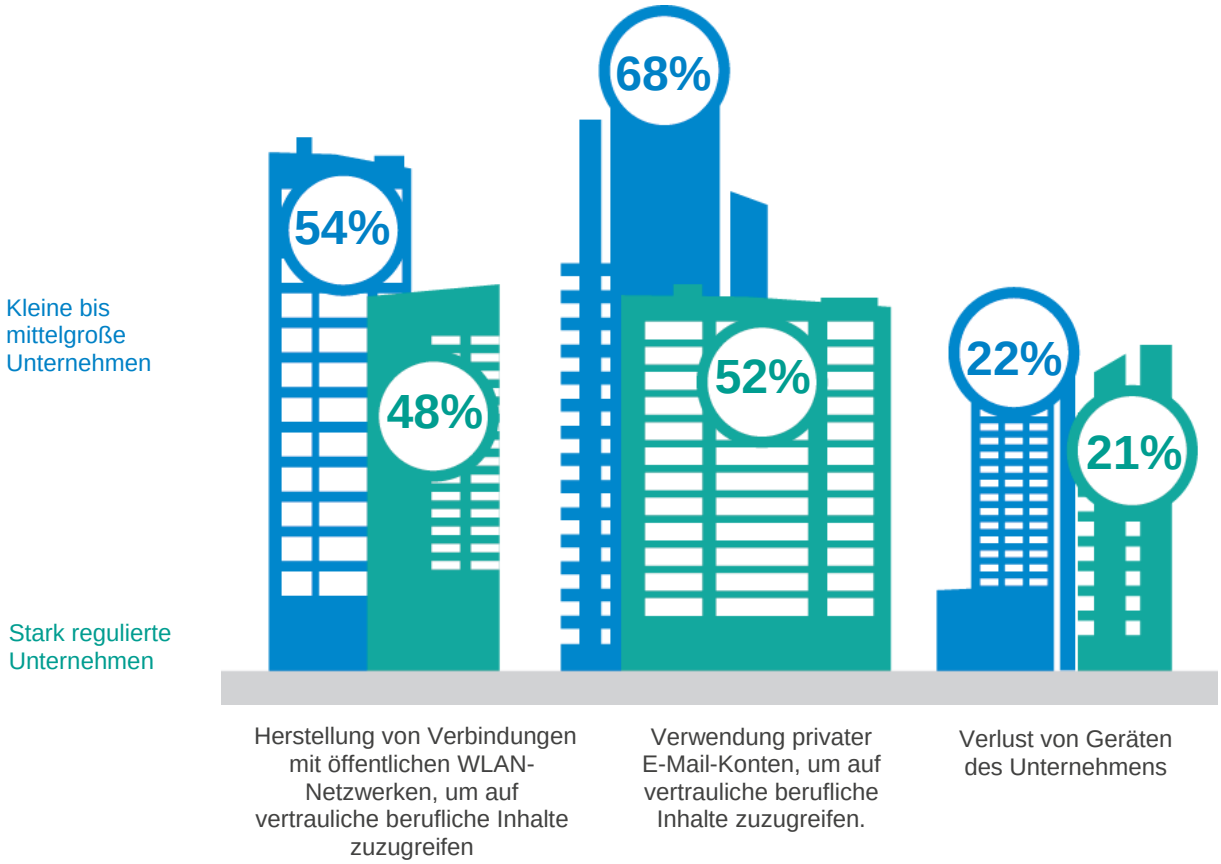
Unsichere Verhaltensweisen am Arbeitsplatz sind häufig

Die Bereitschaft von Mitarbeitern, sensible Daten freizugeben, stellt nicht das primäre Problem dar, das von der Dell Umfrage unter Endbenutzern zum Thema Sicherheit aufgedeckt wurde. Die Tatsache, dass Mitarbeiter auf nicht sichere Weise vertrauliche Daten freigeben oder mit diesen umgehen, ist weitaus besorgniserregender.

45 Prozent der Mitarbeiter in den Unternehmen geben an, während des Arbeitstages nicht sichere Verhaltensweisen zu zeigen. Zu diesen Verhaltensweisen gehören die Herstellung von Verbindungen mit öffentlichen WLAN-Netzwerken, um auf vertrauliche Informationen zuzugreifen (46 Prozent), die Verwendung privater E-Mail-Konten für berufliche Zwecke (49 Prozent) oder der Verlust von Geräten des Unternehmens (17 Prozent). Mitarbeiter in stark regulierten Unternehmen zeigen in sogar noch größerem Umfang nicht sichere Verhaltensweisen: 48 Prozent geben an, Verbindungen zu öffentlichen WLAN-Netzwerken hergestellt haben, um auf vertrauliche berufliche Informationen zuzugreifen; mehr als die Hälfte (52 Prozent) haben private E-Mail-Konten für vertrauliche berufliche Mitteilungen verwendet; und mehr als einer von fünf Mitarbeitern (21 Prozent) hat bereits einmal ein Gerät des Unternehmens verloren. Diese Zahlen sind für Mitarbeiter in kleinen bis mittelgroßen Unternehmen sogar noch höher.

45%

der Mitarbeiter in den Unternehmen geben an, während des Arbeitstages nicht sichere Verhaltensweisen zu zeigen.



Am meisten schockiert hier vielleicht, dass mehr als einer von drei Mitarbeitern (35 Prozent) angibt, dass es allgemeine Praxis sei, beim Verlassen des Unternehmens Unternehmensinformationen mitzunehmen. Diese Situation
erwies sich vor kurzem für Facebook und Uber als problematisch. Die beiden Unternehmen wurden verklagt, weil Führungskräfte von Tochtergesellschaften (Oculus Rift bzw. Otto) Geschäftsgeheimnisse gestohlen haben sollen, als sie ihre vorherigen Arbeitgeber, die Kläger, verließen.[ii] [iii]

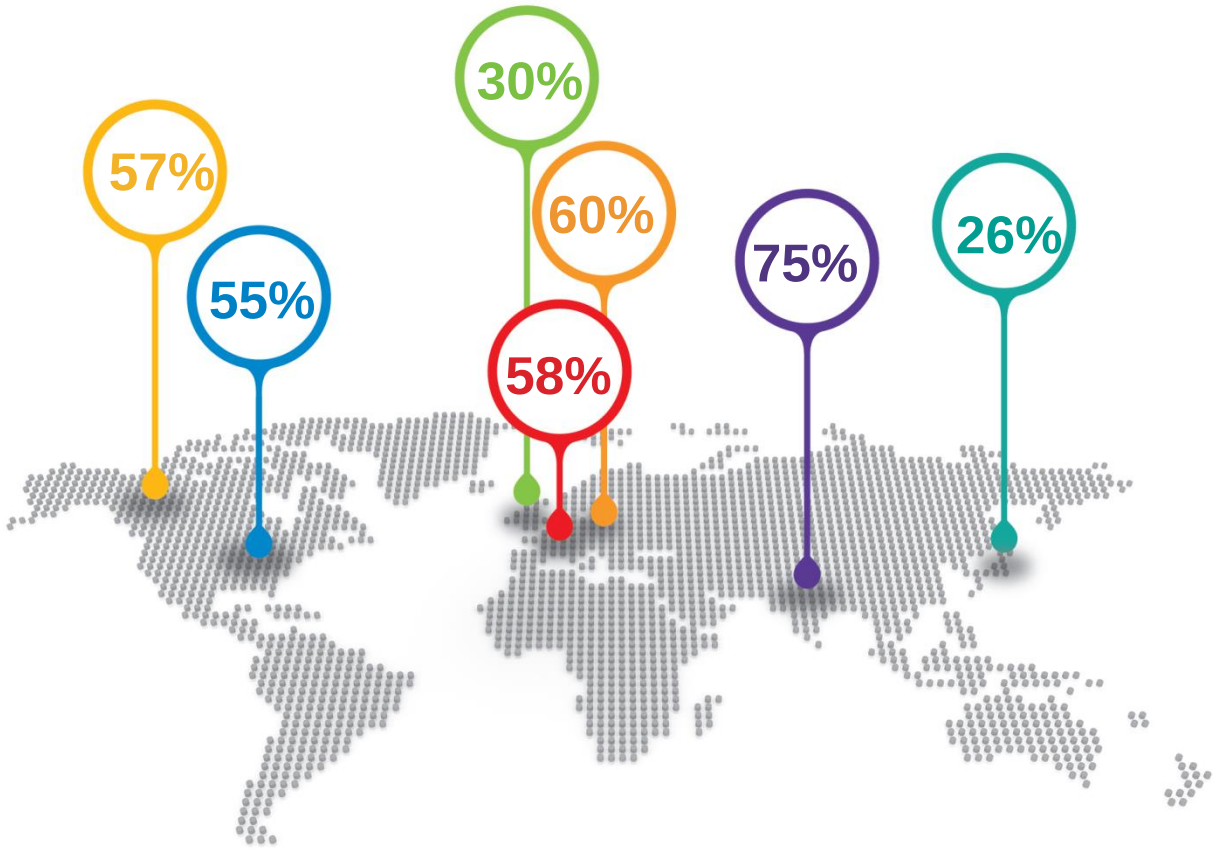
Die Umfrage zeigte, dass kulturelle Unterschiede möglicherweise Einfluss darauf haben, ob Mitarbeiter beim Verlassen
eines Unternehmens Daten mitnehmen. Am häufigsten nehmen Mitarbeiter in Indien (57 Prozent) Unternehmensinformationen mit, während Mitarbeiter in Japan (15 Prozent) dies am seltensten tun. Die meisten Mitarbeiter, die Informationen mitnehmen, nehmen Daten zu Arbeiten mit, die sie selbst ausgeführt haben
(36 Prozent). Immerhin 16 Prozent nehmen jedoch Daten zu Arbeiten mit, die von anderen ausgeführt wurden. In der Regel transportieren Mitarbeiter die Unternehmensdaten auf einem USB-Stick (61 Prozent) oder senden sie per E-Mail (56 Prozent). Beide Verfahren können von Unternehmen nur schwer nachverfolgt oder blockiert werden.

Interessanterweise sagen drei Prozent der Mitarbeiter in allen Unternehmen, die angeben, nicht sichere Verhaltensweisen zu zeigen, dass sie dies in böswilliger Absicht tun. 24 Prozent geben jedoch an, dass sie einfach nur ihre Arbeit erledigen wollten, und 18 Prozent geben an, dass sie nicht wussten, dass ihr Verhalten nicht sicher war. Jedes dieser Szenarien zeigt eine andere problematische Sicherheitslücke auf, die Unternehmen schließen müssen, von Bedrohungen durch Insider bis zum Fehlen effektiver Schulungen zum Thema Sicherheit.

Das Fehlen effektiver Schulungen führt für Unternehmen mit BYOD-Programmen möglicherweise zu noch weitreichenderen Problemen. Von den Mitarbeitern, die private Geräte für den Zugriff auf vertrauliche berufliche Inhalte verwenden, sind 62 Prozent persönlich für die Sicherheit des Geräts verantwortlich. Nur
28 Prozent der Unternehmen weisen diese Verantwortung ihrem IT-Team zu. Wenn sich Mitarbeiter nicht sicher sind, welche Verhaltensweisen risikobehaftet sind, können sie wahrscheinlich nur eingeschränkt für die Sicherheit ihrer privaten Geräte sorgen.

Dasselbe übergreifende Fehlen von Wissen zum Thema Sicherheit hat dazu geführt, dass Cyberangriffe häufig Social Engineering verwenden. Dabei bringt ein Cyberkrimineller Personen dazu, gegen Sicherheitsverfahren zu verstoßen oder sensible Informationen offenzulegen. Cyberkriminelle haben erkannt, dass es für sie einfacher ist, wenn ihre Opfer ihnen ihre Kennwörter verraten, als die Kennwörter ihrer Opfer zu erraten. Der Kriminelle muss nur das Vertrauen oder Interesse seiner Ziele gewinnen, indem er beispielsweise eine lustig wirkende Umfrage entwickelt, die Besucher dazu bringt, sensible Informationen preiszugeben, wie die Straße, in der sie aufgewachsen sind, den Namen ihres ersten Haustieres oder den Mädchennamen ihrer Mutter. Dies ist für Unternehmen besonders deswegen ein Anlass zur Sorge, da beinahe die Hälfte aller Mitarbeiter (49 Prozent) Geräte von Unternehmen verwenden, um auf ihre privaten Konten in Social Media zuzugreifen. Kulturabhängig kann diese Zahl auch höher liegen. In Indien greifen drei von vier Mitarbeitern über Unternehmensgeräte auf private Konten in Social Media zu. Die Zahlen für Mitarbeiter in den USA (55 Prozent), Kanada (57 Prozent), Frankreich (58 Prozent) und Deutschland (60 Prozent) liegen ebenfalls über dem weltweiten Durchschnitt. Andererseits verwenden nur
30 Prozent der Mitarbeiter im Vereinigten Königreich und 26 Prozent der Mitarbeiter in Japan Unternehmensgeräte, um auf private Konten in Social Media zuzugreifen.

49% der Mitarbeiter verwenden Unternehmensgeräte, um auf private Konten in Social Media zuzugreifen.



Mitarbeiter gehen möglicherweise auch unnötige Risiken hinsichtlich der Art und Weise ein, wie sie ihre Arbeit speichern und freigeben. 56 % Prozent der Mitarbeiter nutzen öffentliche Cloud Services wie Dropbox, Google Drive, iCloud und andere, um ihre Arbeit freizugeben oder zu sichern. 53 Prozent verwenden ein privates und nicht ein Unternehmenskonto, um auf Cloud Services zuzugreifen.

Wenn es um die Freigabe vertraulicher Dateien für externe Anbieter oder Berater geht, verwenden 45 Prozent der Mitarbeiter E-Mail. Beinahe ein Drittel (31 Prozent) gibt jedoch an, dass externe Anbieter oder Berater auf das Intranet oder andere interne Informationssysteme ihres Unternehmens zugreifen können. Dies kann sogar noch größere Risiken bergen, wenn der Zugriff dieser externen Anbieter oder Berater nicht korrekt eingeschränkt wird. Wie allgemein bekannt, verzeichnete Target 2014 eine Sicherheitsverletzung, als einem Cyberangreifer mithilfe der Anmeldeinformationen des externen HVAC-Anbieters des Unternehmens der Zugriff auf das Netzwerk des Einzelhändlers gelang.[iv]

Die zunehmende Mobilität der Mitarbeiter in Bezug auf die verwendeten Geräte, die Orte, an denen sie Daten speichern, und die Orte, an denen sie arbeiten, bedeutet auch einen erheblichen Anstieg des Risikos in Bezug auf den Verlust oder den Diebstahl von Daten erheblich. Unternehmen sollten sich nicht nur auf die Standardisierung des Prozesses konzentrieren, anhand dessen festgelegt wird, wann und für wen Daten freigegeben werden dürfen, sondern auch die Art der Freigabe dieser Dateien festlegen und die Maßnahmen definieren, die angewendet werden, wenn ein Mitarbeiter das Unternehmen verlässt.

Mitarbeiterunterstützen den Schutz von Informationen, sind jedoch der Meinung, zu wenig Befugnisse zu haben

Wie die Dell Umfrage unter Endbenutzern zum Thema Sicherheit zeigt, tendieren Mitarbeiter zu einer Art Hassliebe, wenn es um Cybersicherheit am Arbeitsplatz geht. Auf der einen Seite möchten sie nicht, dass die Sicherheit der Daten ihres Unternehmens verletzt wird, und fühlen sich sogar dafür verantwortlich, zum Schutz der Informationen beizutragen. Auf der anderen Seite haben sie jedoch Probleme mit den Einschränkungen, die Sicherheitsprogramme ihren alltäglichen Tätigkeiten auferlegen können.

Beinahe zwei von drei Mitarbeitern (65 Prozent) sind der Meinung, dass es in ihrer Verantwortung liegt, vertrauliche Daten zu schützen, einschließlich der Beschaffung von Informationen zu möglichen Risiken und der Anwendung von Verhaltensweisen, die ihr Unternehmen schützen. Nur 36 Prozent der Mitarbeiter sind jedoch sehr zuversichtlich, wenn es um ihr Wissen darüber geht, wie sie sensible Unternehmensinformationen schützen können.

Die Mehrzahl der Mitarbeiter ist zwar der Ansicht, dass es in ihrer Verantwortung liegt, Unternehmensinformationen zu schützen, sieht sich diesbezüglich jedoch einer Reihe von Hindernissen gegenüber. 21 Prozent geben an, dass ihre Arbeit durch die von der IT eingerichteten Sicherheitsverfahren verlangsamt wird, während 21 Prozent der Ansicht sind, dass es schwierig ist, mit sich ständig verändernden Sicherheitsanleitungen und -richtlinien Schritt zu halten. Mitarbeiter geben sogar an, dass sie sich Gedanken über ihre fehlende Fähigkeit machen, Unternehmensdaten effektiv zu schützen. 22 Prozent geben an, dass sie sich Sorgen machen, eines Tages das Falsche zu tun und dem Unternehmen einen echten Schaden zuzufügen.

Auch wenn sie sich in Bezug auf den Schutz vertraulicher Daten persönlichen Herausforderungen gegenübersehen, sind mehr als drei von vier Mitarbeitern (76 Prozent) auch der Meinung, dass ihr Unternehmen die Sicherheit auf Kosten der Mitarbeiterproduktivität priorisiert. Auch wenn Mitarbeiter der Meinung sind, dass sie durch Sicherheitsverfahren behindert werden, geben sie dennoch an, nicht zu wissen, wie sie sensible Informationen schützen können.

Schulungen scheinen eine klare Lösung für das Fehlen von Wissen zum Thema Sicherheit und das Fehlen der entsprechenden Zuversicht darzustellen.
Während beinahe zwei von drei Mitarbeitern (63 Prozent) an Schulungen zum Thema Cybersicherheit im Zusammenhang mit dem Schutz sensibler Daten teilnehmen müssen, zeigen 18 Prozent der Mitarbeiter nicht sichere Verhaltensweisen
am Arbeitsplatz, ohne zu erkennen, dass sie etwas falsch gemacht haben. Außerdem zeigten 24 Prozent der Mitarbeiter, die an Schulungen zum Thema Cybersicherheit teilgenommen haben, nicht sichere Verhaltensweisen, weil sie einfach nur
ihre Arbeit erledigen wollten.

Für dieses Problem gibt es keine Einheitslösung, da sich die Anforderungen in Bezug auf die Sicherheit in den einzelnen Unternehmen unterscheiden. Es ist jedoch klar, dass sich Unternehmen und Mitarbeiter irgendwo in der Mitte treffen müssen. Auch wenn viele Mitarbeiter bereits an Schulungen zum Thema Cybersicherheit teilnehmen, benötigt das Management möglicherweise auch eine "Schulung" durch Mitarbeiter, um die alltäglichen Aufgaben der Mitarbeiter umfassend zu verstehen und mehr über die Szenarien zu erfahren, in denen sich Mitarbeiter berechtigt fühlen, vertrauliche Daten freizugeben.

Wichtigste Punkte

Unter all den Ergebnissen dieser Umfrage enttäuscht vielleicht die Tatsache am meisten, dass beinahe zwei von drei Mitarbeitern, die mit vertraulichen Daten befasst sind, zwar an Schulungen zum Thema Cybersicherheit teilnehmen, aber dennoch nicht wissen, wie sie sensible Informationen schützen können. Auch wenn sie die Best Practices kennen, sind sie bereit, sie absichtlich zu übersehen, wenn dies notwendig ist, um ihre Arbeit zu erledigen.

Dies weist auf ein wesentliches Problem hin: Unternehmensrichtlinien zu Nutzung und Freigabe vertraulicher Daten sind entweder unklar oder nicht umfassend genug, um das gesamte Spektrum alltäglicher Szenarien abzudecken, mit denen es Mitarbeiter am Arbeitsplatz zu tun haben. Unternehmen müssen aufhören, Mitarbeitern einfach zu sagen, dass sie vertrauliche Informationen nicht freigeben dürfen. Stattdessen müssen sie ihnen ermöglichen, vertrauliche Daten freizugeben, wenn dies sinnvoll ist, jedoch auf sichere und einfache Weise.

Unternehmen können diese Herausforderungen nur bewältigen, wenn sie einen höheren Grad an Bewusstsein, Befähigung und Schutz gleichzeitig anstreben.

- Entwickeln Sie einfache und klare Richtlinien und stellen Sie sicher, dass diese die Behandlung häufiger Szenarien beschreiben, denen sich Mitarbeiter gegenübersehen. Richtlinien sind der Schlüssel zur Verhinderung von Sicherheitsverletzungen und Datenverlusten. Unternehmen müssen jedoch zuerst identifizieren, was für sie wichtig ist, sowohl in Bezug auf Endgeräte als auch in Bezug auf kritische Daten, und Richtlinien erstellen, die den Endbenutzerzugriff, die Arten von Daten, die Personen, die auf die Daten zugreifen können, und die Regeln für die Verbreitung außerhalb des Unternehmens definieren. Das Ziel besteht darin, dass schließlich mindestens 99 Prozent der Mitarbeiter verstehen, warum Sicherheit wichtig ist, und ihr Bestes geben, um die Richtlinien während des Tages einzuhalten, unabhängig vom verwendeten Gerät, dem Ort, an dem sie arbeiten, oder den Personen, mit denen sie arbeiten.

- Nutzen und unterstützen Sie Produktivität. Die sicherste Umgebung ist eine Umgebung, die keine Verbindung mit dem Internet hat. Das ist natürlich keine realistische Vorstellung. Sicherheit und Produktivität müssen zusammengeführt werden. Wenn die Richtlinien für die Datensicherheit die Dynamik der Mitarbeiter beeinträchtigen, werden Mitarbeiter Wege finden, sie zu umgehen. Sicherheit sollte geschäftliche Initiativen nicht einschränken, sondern sie durch eine bessere Ausrichtung zwischen der Führungsebene und den IT-Teams des Unternehmens unterstützen. Dieses perfekte Gleichgewicht muss erreicht werden, auch wenn es von Unternehmen zu Unternehmen unterschiedlich sein kann,

- Nutzen Sie Sicherheitslösungen, die Daten ortsunabhängig schützen. Unternehmen müssen Daten nicht nur auf PCs und Mobilgeräten schützen, sondern auch, wenn sie über die Cloud freigegeben, an ein privates E-Mail-Konto gesendet oder zu einem externen Gerät übertragen werden. Der Schutz von Daten setzt eine umfassende Lösung voraus – eine Lösung, die die Daten ortsunabhängig schützen, kontrollieren und überwachen kann. Unternehmen müssen in der Lage sein, zu steuern, wer Zugriff auf die Daten erhalten kann; zu überwachen, wo sich die Daten befinden und wie sie verwendet werden; und Rechte und Richtlinien anzuwenden, sodass nur die richtigen Personen in den richtigen Umständen auf die Daten zugreifen können. Die Bereitstellung einer robusten und mehrschichtigen Sicherheitsinfrastruktur, die Daten

schützt, ohne Abläufe und die Mitarbeiterproduktivität zu beeinträchtigen, bewahrt Unternehmen vor Datenverlusten.

Die Dell Umfrage unter Endbenutzern zum Thema Sicherheit zeigt, dass Unternehmen zwei Wahrheiten akzeptieren müssen: Vertrauliche Daten werden täglich versendet, gespeichert und verwendet werden und Mitarbeiterschulungen alleine reichen nicht aus, um die Sicherheit von Unternehmensinformationen zu gewährleisten. Sicherheitsprogramme von Unternehmen müssen eine Kombination von Lösungen enthalten, die darauf ausgerichtet sind, das Sicherheitsbewusstsein der Mitarbeiter, die Befähigung der Mitarbeiter und den Schutz durch die Mitarbeiter zu stärken. Wenn Unternehmen ihre Daten angesichts der sich ständig weiterentwickelnden Bedrohungslandschaft wirklich schützen möchten, benötigen sie klare Protokolle, die vor dem Hintergrund eines realistischen Verständnisses der alltäglichen Aufgaben ihrer Mitarbeiter. entwickelt wurden. Darüber hinaus müssen sie Technologien anwenden, die sensible Daten überall schützen – im Datenspeicher, während der Übertragung oder während der Verwendung.

Methodik

Dimensional Research führte im Auftrag von Dell Data Security eine Umfrage unter 2.608 Mitarbeitern in Unternehmen mit mindestens 250 Mitarbeitern durch, die persönlich Zugriff auf vertrauliche, sensible oder regulierte Daten und Informationen haben und mit diesen arbeiten. Die Teilnehmer stammten aus acht Ländern: Australien, Deutschland, Frankreich, Indien, Kanada Japan, Vereinigtes Königreich und Vereinigte Staaten. Die Umfrage wurde zwischen dem 24. Februar 2017 und dem 9. März 2017 durchgeführt.

Über Dimensional Research

Dimensional Research stellt praxisbezogene Marktstudien bereit, um Technologieunternehmen zu helfen, intelligentere geschäftliche Entscheidungen zu treffen. Unsere Mitarbeiter sind Technologieexperten und verstehen, wie IT-Abteilungen in Unternehmen funktionieren. Unsere Forschungsservices ermöglichen ein klares Verständnis von Kunden und Marktdynamiken. Weitere Informationen finden Sie auf www.dimensionalresearch.com.

Über Dell Inc.

Mit preisgekrönten Desktops, Notebooks, 2-in-1-Geräten, Thin Clients, leistungsfähigen Arbeitsstationen, robusten Geräten für spezielle Umgebungen, Monitoren, Lösungen für die Endpunktsicherheit und Services bietet Dell den Mitarbeitern von heute alles, was sie benötigen, um auf sichere Weise Verbindungen herzustellen, produktiv zu sein und zusammenzuarbeiten – überall und jederzeit. Dell, Teil von Dell Inc., stellt Kunden von Verbrauchern bis zu Unternehmen aller Größenordnungen ein äußerst umfassendes und innovatives Endbenutzerportfolio bereit.

---

[i] "Leading banks in the United States as of December 31, 2016, by number of employees", Statista, https://www.statista.com/statistics/250220/ranking-of-united-states-banks-by-number-of-employees-in-2012/

[ii] Selena Larson, "Facebook loses $500 million Oculus lawsuit", CNN Money, 2. Februar 2017, http://money.cnn.com/2017/02/01/technology/zenimax-oculus-lawsuit-500-million/

[iii] Reuters, "Uber to Push for Arbitration in Waymo Trade Secrets Theft Case", Fortune, 16. März 2017, http://fortune.com/2017/03/16/uber-arbitration-waymo/

[iv] "Target Hackers Broke in Via HVAC Company", Krebson Security, 5. Februar 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/