FORRESTER®

Ein Profil zur Einführung benutzerdefinierter Technologien im Auftrag von Dell | Oktober 2017

Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

BEGINNEN ▶

Ein Profil zur Einführung benutzerdefinierter Technologien im Auftrag von Dell | Oktober 2017

Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

Sicherheit sollte schützen und befähigen

Um mit dem Wachstum der geschäftlichen Mobilität Schritt zu halten, ohne dabei den potenziellen Risiken zu erliegen, muss die IT in der Lage sein, komplexe Probleme wie Servicebereitstellung, Gerätebeschaffung und Sicherheitsüberwachung effizient anzugehen. Warum? Information Worker benötigen in einer Vielzahl von Geschäftsanwendungen und -geräten Zugriff auf häufig vertrauliche Informationen, unabhängig von ihrem Standort. Mit anderen Worten: Sicherheits- und Datenschutzrichtlinien, die die Produktivität der Endbenutzer nicht beeinträchtigen, werden die Mitarbeiter stärken und ihre Leistung steigern.

HINTERGRUND DES PROJEKTS

Im Juli 2017 beauftragte Dell Forrester mit einer Studie über die Arbeitskräfte des 21. Jahrhunderts und darüber, wie ihre neuen Gewohnheiten, Einstellungen und Arbeitsformen die Arbeitswelt neu gestalten. Durch die steigende Zahl an Mitarbeitern sind die Unternehmen nicht mehr in der Lage, den Anforderungen ihrer Mitarbeiter ausreichend gerecht zu werden. Um ihre Aufgaben erledigen zu können, umgehen die Mitarbeiter die Sicherheitsrichtlinien, um sich bei Bedarf das zu beschaffen, was sie gerade benötigen. Unternehmen müssen die unterschiedlichen Verhaltensweisen der Belegschaft verstehen und die Sicherheitsbedürfnisse sorgfältig und gleichgewichtig abwägen. Ansonsten laufen sie Gefahr, sich bestehenden und neuen Bedrohungen aussetzen.

Land

- Australien: **25 %**
- Indien: **25 %**
- USA: **25 %**
- Großbritannien: **25 %**

Unternehmenstyp

- Lokal: **11 %**
- Regional: **35 %**
- Multinational: **54 %**

Jahresumsatz (USD)

- 400 bis 499 Mio. USD: **21 %**
- 500 bis 999 Mio. USD: **31 %**
- 1 bis 5 Mrd. USD: **28 %**
- > 5 Mrd. USD: **20 %**

Arten von Mitarbeitern

- Mitarbeiter im Büro: Büro-Mitarbeiter: **32 %** und „Flurkrieger“: **23 %**
- Mitarbeiter ohne Büroarbeitsplatz: Business-Traveller: **24 %** Home-Office-Mitarbeiter: **22 %**
- **Sonderfunktion:** Wissensarbeiter: Kreativarbeiter: **30 %** und Techniker: **24 %**

Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

Die vielfältige Belegschaft verwendet heutzutage viele Geräte

Die Digitalisierung des Arbeitsplatzes befähigt Information Worker, bei Bedarf jederzeit und von überall die Informationen zu beschaffen, die sie benötigen. Die Tage des pflichtbewussten Mitarbeiters, der täglich vom und zum selben Ort pendelt, sind vorbei. Die Verbreitung mobiler Technologien, flexible Arbeitsrichtlinien und die Vorlieben der Mitarbeiter führen dazu, dass die digitale Belegschaft heute von zu Hause, an öffentlichen Orten und an mehreren Standorten arbeitet. Information Worker verwenden zudem eine Vielzahl von Geräten. Die Herausforderung besteht darin, dass die IT ihren Mitarbeitern hilft, diese Geräte sicher zu verwenden, um die IT-eigenen Sicherheitsprotokolle zu erfüllen und das Unternehmen effizienter und erfolgreicher zu machen, ohne die Autonomie oder Produktivität der Mitarbeiter zu beeinträchtigen.

Für diese Studie haben wir folgende Arten von Mitarbeitern definiert:

- **Mitarbeiter im Büro:** Überwiegend am Schreibtisch tätig und „Flurkrieger“.
- **Mitarbeiter ohne Büroarbeitsplatz:** Telearbeiter und mobile Fachkräfte.
- **Wissensarbeiter:** Kreativarbeiter und Techniker.

Laptops sind immer noch das beliebteste Gerät bei allen Arten von Mitarbeitern. Durchschnittlich nutzen 57 % sie, um ihre Arbeit zu erledigen, egal wo sie arbeiten.

„Wo verwenden Sie in der Regel die folgenden Geräte für die Arbeit?“

	Home-Office-Mitarbeiter	Business-Traveller	Büro-Mitarbeiter	Meeting-Spezialisten	Kreativar-beiter	Engineer worker
Jede Art von Desktop-PC	58 %	45 %	67 %	63 %	58 %	53 %
Jede Art von Laptop	69 %	50 %	63 %	38 %	61 %	63 %
Jede Art von 2-in-1-/„Convertible“-PC mit Touchscreens und schwenkbaren Bildschirmen	26 %	34 %	17 %	23 %	33 %	38 %
Jede Art von gemeinsam genutztem Arbeitsbereich	20 %	28 %	16 %	22 %	31 %	19 %
Jede Art von Ad-hoc-Monitor für die Teamarbeit	19 %	20 %	17 %	12 %	24 %	20 %
Jede Art von portablen Datenträgern und Zubehör	21 %	34 %	26 %	21 %	36 %	32 %
Jede Art von 7-bis 12-Zoll-Tablets	17 %	35 %	20 %	18 %	27 %	28 %
Mobiltelefon	13 %	22 %	6 %	6 %	15 %	14 %
Smartphone	56 %	64 %	57 %	41 %	70 %	59 %
Zweckgebundenes mobiles Gerät	10 %	16 %	5 %	18 %	9 %	10 %

Grundlage: 400 Informationsarbeiter aus allen Branchen in den USA, Großbritannien, Indien und Australien
Quelle: Eine von Dell in Auftrag gegebene Studie von Forrester Consulting, September 2017

Ein Profil zur Einführung benutzerdefinierter Technologien im Auftrag von Dell | Oktober 2017

Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

Mitarbeiter empfinden die Sicherheitsprozesse ihrer Firma als reaktiv

Daten sind der Lebensnerv der heutigen digitalen Unternehmen. Der Schutz vor Diebstahl, Missbrauch und Übergriffen ist für Unternehmen auf der ganzen Welt oberste Priorität, zumal Firmen nicht in die Ferne blicken oder die Nachrichten verfolgen müssen, um zu wissen, dass Datenbedrohungen immer häufiger werden.

Information Worker gaben an, dass eine Sicherheitsverletzung zu mehr Ausgaben, mehr Sicherheitsprojekten und mehr Vorschriften führen würde. Beispielsweise gaben die Befragten an, dass aufgrund einer Sicherheitsverletzung mehr Sicherheits- und Auditanforderungen (72 %), höhere Ausgaben für Prävention (67 %) und höhere Ausgaben für Erkennungstechnologien (65 %) anfallen würden.

Darüber hinaus würde eine Sicherheitsverletzung nicht nur unternehmensweite Aufmerksamkeit erzeugen, sondern sie würde sich auch direkt auf das Geschäft auswirken, da die Marke geschädigt (62 %) und es zu Reputationsproblemen (59 %) kommen würde.

82 % der Information Worker bewerteten die Reaktion ihres Unternehmens auf eine Sicherheitsverletzung als sehr reaktionsschnell oder reaktionsschnell.

„Was denken Sie, würde am ehesten im Falle oder in Folge einer Sicherheitsverletzung geschehen?“ (Dargestellt sind nur die Top 5 von „sehr wahrscheinlich“ und „wahrscheinlich“)

Grundlage: 400 Informationsarbeiter aus allen Branchen in den USA, Großbritannien, Indien und Australien
Quelle: Eine von Dell in Auftrag gegebene Studie von Forrester Consulting, September 2017

Ein Profil zur Einführung benutzerdefinierter Technologien im Auftrag von Dell | Oktober 2017

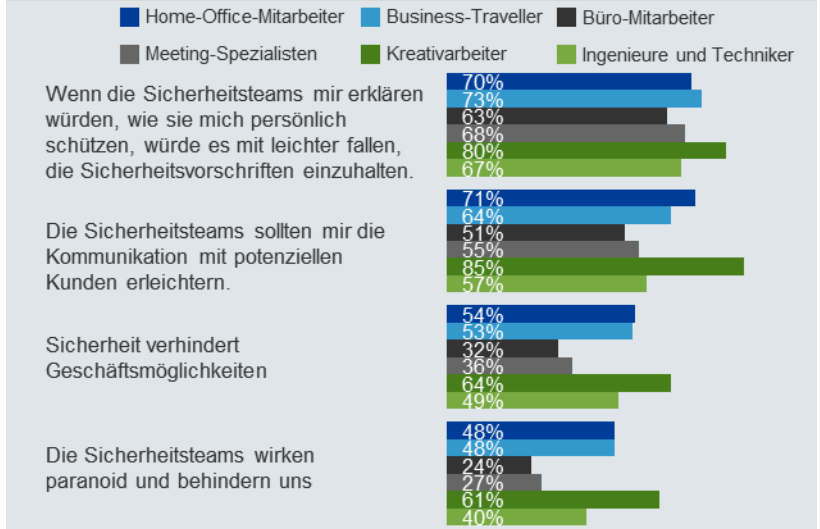
Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

Coaching, nicht Controlling, führt zu besseren Sicherheitspraktiken

Unternehmen haben Schwierigkeiten zu erfassen, wer und was ihre Belegschaft umfasst, und die verschiedenen Kombinationen von Mitarbeitertypen zu managen. Alle Arten von Mitarbeitern stimmen voll zu oder stimmen zu, dass die Sicherheitsteams ihnen erklären sollten, wie sie zu ihrem Schutz beitragen. Dies würde dazu führen, dass sie die Sicherheitsmaßnahmen eher umsetzen.

Jedoch gibt es einige interessante Unterschiede zwischen den Mitarbeitertypen. Mitarbeiter ohne Büroarbeitsplatz (durchschnittlich 54 %) und Wissensarbeiter (im Durchschnitt 57 %) gaben an, dass Sicherheitsmaßnahmen Geschäftsmöglichkeiten im Wege ständen und dass es für die Mitarbeiter leichter sein sollte, mit potenziellen Kunden zu kommunizieren. Darüber hinaus müssen Sicherheitsteams in der Lage sein, die Verwendung verschiedener Geräte für Mitarbeiter zu unterstützen und sogar zu beschleunigen. Mitarbeiter ohne Büroarbeitsplatz und Wissensarbeiter gaben jedoch an, dass sie Schwierigkeiten hätten, mit ihren Sicherheitsteams zusammenzuarbeiten: Sie seien paranoid und würden sie von ihrer Arbeit abhalten.

„Inwieweit stimmen Sie den folgenden Aussagen über die Teams, die für die Sicherheitsrichtlinien der Geräte zuständig sind, die Sie für Ihre Arbeit einsetzen, zu?“ Dargestellt sind nur „Stimme voll zu“ oder „Stimme zu“)



Grundlage: 400 Informationsarbeiter aus allen Branchen in den USA, Großbritannien, Indien und Australien
Quelle: Eine von Dell in Auftrag gegebene Studie von Forrester Consulting, September 2017

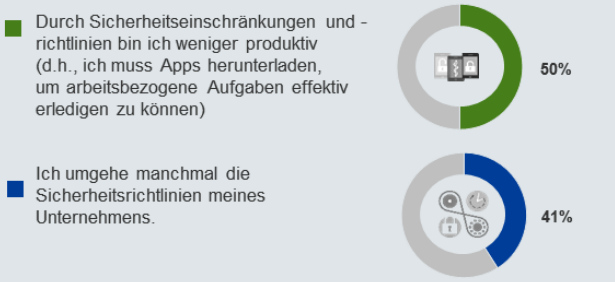
Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

Mitarbeiter werden durch die Richtlinien ihres Unternehmens ausgebremst

Die Mitarbeiter versuchen, ihre Arbeit zu erledigen, aber Sicherheitsmaßnahmen halten sie davon ab, ihre Aufgaben effektiv zu erfüllen, weil diese schlecht konzipiert sind und weil sie nicht dynamisch genug sind, um auf die unterschiedlichen Arten von Mitarbeitern und ihre Bedürfnisse einzugehen. Dies erklärt, warum die Hälfte (50 %) der Information Worker angaben, Sicherheitsbeschränkungen und -richtlinien schränkten ihre Produktivität ein, und 41 % äußerten, dass sie die Sicherheitsrichtlinien des Unternehmens manchmal umgingen.

Mit anderen Worten: Mitarbeiter wählen den Weg des geringsten Widerstandes, um ihre Arbeit zu erledigen, weil dieser der wirkungsvollste ist (57 %). Mitarbeiter benötigen und fordern von ihren Geräten aus Zugang zu sensiblen Unternehmensinformationen, und die Erteilung von Genehmigungen durch die IT ist ein langer und mühsamer Prozess (37 %). Interessanterweise verstoßen Mitarbeiter ohne festen Büroarbeitsplatz sowie Wissensarbeiter eher gegen das Sicherheitsprotokoll, um die Informationen zu bekommen, die sie benötigen. Zum Beispiel verstoßen 75 % der mobilen Fachkräfte und Wissensarbeiter sowie Techniker (49 %) und Kreative (52 %) häufiger gegen die Sicherheitsrichtlinien. Daher sollten sich Unternehmen auf sie konzentrieren, da hier ein größeres Risiko besteht.

„Wie sehr stimmen Sie dem Folgenden zu?“ („Stimme voll zu“ und „Stimme zu“ sind in der Darstellung zusammengefasst)



Grundlage: 400 Informationsarbeiter aus allen Branchen in den USA, Großbritannien, Indien und Australien
Quelle: Eine von Dell in Auftrag gegebene Studie von Forrester Consulting, September 2017

„Warum umgehen Sie manchmal die Sicherheitsrichtlinien Ihres Unternehmens?“ (Wählen Sie alle zutreffenden Antworten aus.)

Grundlage: Variabel; Informationsarbeiter aus allen Branchen in den USA, Großbritannien, Indien und Australien
Quelle: Eine von Dell in Auftrag gegebene Studie von Forrester Consulting, September 2017

Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

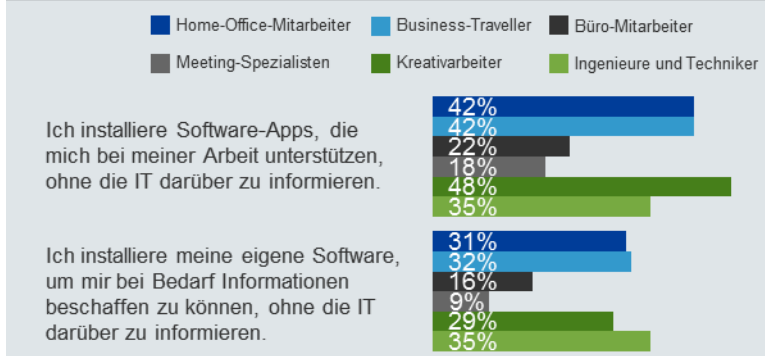
Mitarbeiter wollen produktiv sein, nicht bösartig

Mitarbeiter möchten Zugang zu Software und Apps, um ihre Arbeit erledigen zu können. Wenn Sicherheitsteams ihnen zu viele Richtlinien und Kontrollen in den Weg stellen, z. B. beim Zugriff auf eine App oder beim Download von Software, suchen sie aktiv nach Alternativen aus anderen Quellen, umgehen Sicherheitsprozesse – ohne IT-Kenntnisse – und erhöhen so das Sicherheitsrisiko. Die Mitarbeiter tun dies jedoch nicht in böswilliger Absicht ausgeführt. Sie brauchen im konkreten Fall Zugang zu Apps und Software, um produktiv arbeiten zu können.

Es überrascht nicht, dass Büroangestellte (überwiegend am Schreibtisch Tätige sowie „Flurkrieger“) seltener Software oder Apps installieren, ohne dass die IT-Mitarbeiter dies wissen, als ihre Kollegen außerhalb des Büros (Telearbeiter und mobile Mitarbeiter) und Wissensarbeiter (Kreative und Techniker). Sie tun dagegen eher, was sie wollen, wenn sie dadurch produktiver sind und jederzeit und von überall Zugang zu Informationen haben.

Es gibt klare Sicherheitslücken: *62 % der Telearbeiter befürchten, für eine Sicherheitsverletzung oder ein Sicherheitsereignis verantwortlich gemacht zu werden. Techniker sind besorgt darüber, dass Kundendaten verloren gehen könnten (73 %). Dennoch haben sie das Gefühl, dass sie zur Steigerung ihrer Produktivität Apps installieren müssen, auch wenn die IT nichts davon weiß.*

„Wie würden Sie vorgehen, um die Software zu bekommen, die Sie für Ihre Arbeit benötigen?“
(Bitte nur eine Antwortmöglichkeit auswählen.)



Grundlage: 400 Informationsarbeiter aus allen Branchen in den USA, Großbritannien, Indien und Australien
Quelle: Eine von Dell in Auftrag gegebene Studie von Forrester Consulting, September 2017

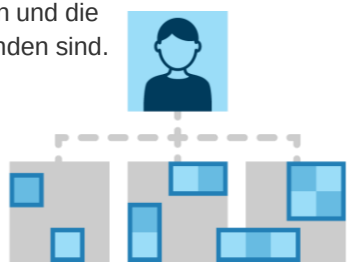
Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

Mitarbeiter müssen Daten teilen: Die IT sollte ihnen dies auf sichere Weise ermöglichen

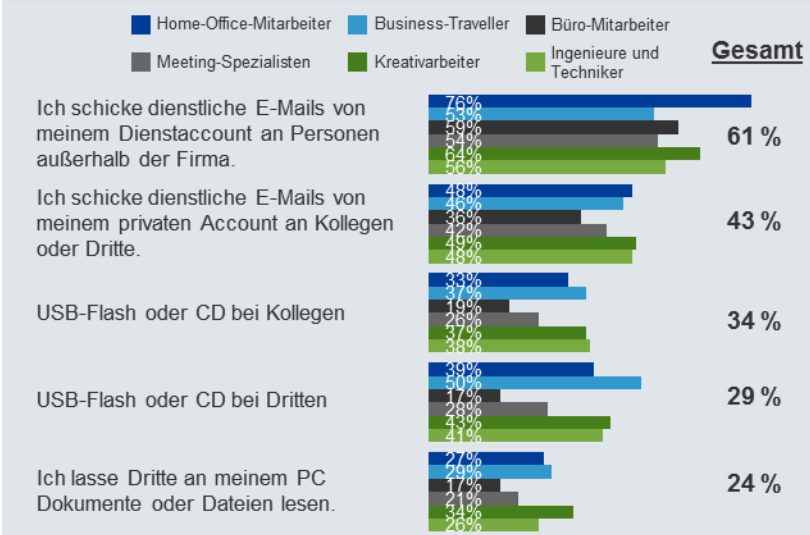
Im 21. Jahrhundert ist die Datenwirtschaft von entscheidender Bedeutung, um zu verstehen, dass Daten ein Eigenleben haben. Unternehmen sammeln Datenberge, was bedeutet, dass die Notwendigkeit, diese Daten zu schützen, aufgrund der Datenmengen, die von den Endnutzern erzeugt und an verschiedenen Orten wie Cloud, USB-Sticks usw. gespeichert und dupliziert werden, zunimmt.

Obwohl sich die Mitarbeiter der Auswirkung und Bedeutung einer Sicherheitsverletzung bewusst sind, wollen, müssen und werden sie Daten mit Kollegen oder Drittunternehmen teilen. Die Mitarbeiter teilen diese Informationen jedoch in unsicheren Umgebungen und setzen das Unternehmen so einem Risiko aus. Sicherheitsfachleute müssen Lösungen finden, die die verschiedenen Arten von Mitarbeitern heute in einer viel sichereren Weise unterstützen und die leicht zugänglich und nahtlos zu verwenden sind.

71 % der Mitarbeiter gaben an, dass sie Dateien täglich oder wöchentlich mit Dritten teilen.



„Wie teilen Sie Dokumente oder Dateien mit Dritten?“
(Wählen Sie alle zutreffenden Antworten aus.)



Grundlage: 400 Informationsarbeiter aus allen Branchen in den USA, Großbritannien, Indien und Australien
Quelle: Eine von Dell in Auftrag gegebene Studie von Forrester Consulting, September 2017

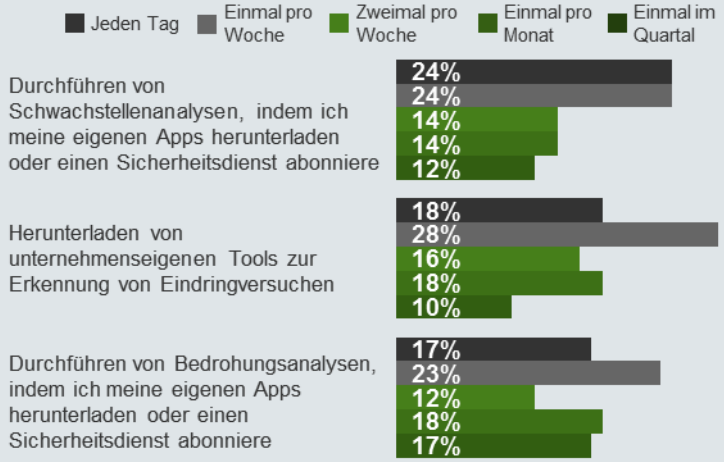
Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

Mit der nötigen Autorität und den entsprechenden Tools würden die Mitarbeiter die Sicherheit selbst in die Hand nehmen

Es lässt sich nicht leugnen, dass die gegenwärtigen Sicherheitskonzepte extrem fragmentiert sind, wenn man sich die verschiedenen Arten von Mitarbeitern ansieht. Mitarbeiter schätzen Sicherheit, aber sie möchten, dass diese Sicherheit sie bei ihren täglichen Aufgaben weniger stört. Je weniger die Sicherheit als störend empfunden wird, desto offener sind die Mitarbeiter dafür. Wenn die IT jedoch ihre Produktivität durch Authentifizierungsprozesse einschränkt oder Einschränkungen für bestimmte Apps und Tools festlegt, die die Mitarbeiter benötigen, um ihre Arbeit effektiv zu erledigen, werden sich die Mitarbeiter nomadisch verhalten.

Die Mitarbeiter verstehen jedoch auch, dass Sicherheit keine leichte Aufgabe ist. Ihre Einstellungen ändern sich, weil sie Verständnis für die Sicherheitsteams haben. Dies erklärt, warum die Mitarbeiter angesichts der Kontrolle zumindest monatlich Schwachstellenanalysen durchführen würden. Ziel ist es, die richtige Balance zu finden zwischen einer zu strengen Kontrolle der Mitarbeiter einerseits und einer nicht als störend empfundenen Sicherheitspolitik andererseits. Die Einbettung von Dateischutz in den natürlichen Ablauf von Arbeitsprozessen und die Installation von Malwareschutz sind der Schlüssel für die Produktivität und Sicherheit der Mitarbeiter. Eine Vielzahl von Sicherheitslösungen kann diese Verhaltensdaten nutzen, um potenzielle Bedrohungsaktivitäten auf anderen Ebenen (Endpunkt, Netzwerk, physisch/geografisch) zu korrelieren oder fundiertere Entscheidungen über die Risiken einer bestimmten Transaktion oder eines bestimmten Verhaltens zu treffen.

„Wenn Sie für die Gewährleistung Ihrer eigenen Sicherheit selbst verantwortlich wären, wie oft würden Sie dann die folgenden Dinge tun?“



Grundlage: 400 Informationsarbeiter aus allen Branchen in den USA, Großbritannien, Indien und Australien
Quelle: Eine von Dell in Auftrag gegebene Studie von Forrester Consulting, September 2017

Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

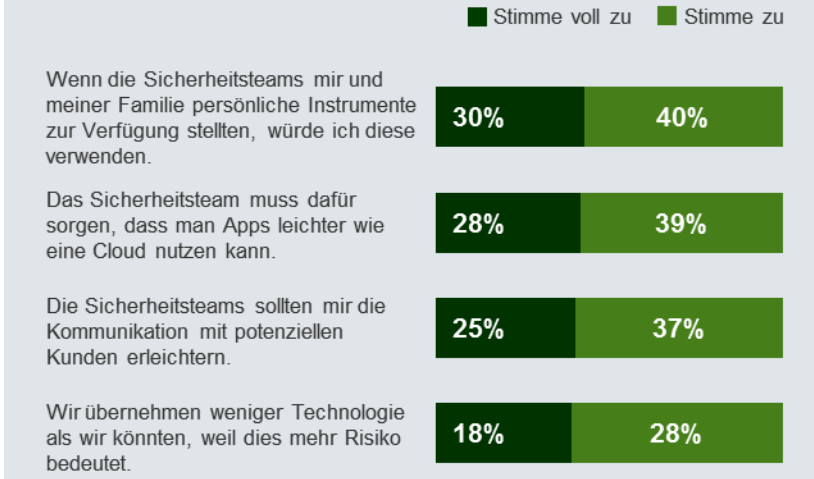
Sicherheitsteams können durch die Bereitstellung der richtigen Tools zur Mitarbeiterbefähigung beitragen

Technologische Vielfalt und sich verändernde Arbeitsmethoden öffnen einer Vielzahl von Sicherheitsproblemen die Tür, die die Marke und die Sicherheit Ihres Unternehmens bedrohen. Zum Beispiel wird ein erhöhter Bedarf der Mitarbeiter an Anwendungen und Daten die Sicherheitsteams dazu veranlassen, sicherzustellen, dass neue Mitarbeitertechnologie keine sensiblen Informationen gefährdet, autorisierten Mitarbeitern aber uneingeschränkten Zugriff ermöglicht, unabhängig davon, ob das Unternehmen die verwendeten Geräte besitzt.

Es ist daher keine Überraschung, dass sich die Mitarbeiter persönliche Sicherheitstools (70 %) und Zugriff auf Apps in der Cloud (67 %) wünschen. Durch die Bereitstellung von Sicherheitstools für alle Arten von Mitarbeitern können diese beim Zugriff auf vertrauliche Informationen vorsichtiger vorgehen.

Unternehmen, die nach Sicherheitslösungen suchen, die es den Mitarbeitern ermöglichen, effektiv und sicher zusammenzuarbeiten, schützen das Unternehmen langfristig. Um die Sicherheit zu verbessern, ohne die Produktivität und die Geschäftsergebnisse zu beeinträchtigen, sollten Sicherheitsexperten die Mitarbeiter durch Tools und Anleitungen in die Lage versetzen, auf sich selbst aufzupassen. Die Rolle der IT-Sicherheitsteams sollte darin bestehen, den Mitarbeitern zu vertrauen, aber auch die Dinge zu überprüfen.

„Inwieweit stimmen Sie den folgenden Aussagen über die Teams, die für die Sicherheitsrichtlinien der Geräte zuständig sind, die Sie für Ihre Arbeit einsetzen, zu?“
(Dargestellt sind nur „Stimme voll zu“ und „Stimme zu”)



Grundlage: 400 Informationsarbeiter aus allen Branchen in den USA, Großbritannien, Indien und Australien
Quelle: Eine von Dell in Auftrag gegebene Studie von Forrester Consulting, September 2017

Ein Profil zur Einführung benutzerdefinierter Technologien im Auftrag von Dell | Oktober 2017

Sicherheitsentwicklung für die Ansprüche des modernen Mitarbeiters

Alle Mitarbeiter betrachten: Sicherheitsbedürfnisse für eine bessere Mitarbeitererfahrung

Die Technologie verändert, wie und wo Mitarbeiter arbeiten. Sicherheitsteams müssen auf dem Laufenden bleiben und den verschiedenen Arten von Mitarbeitern gerecht werden. Die Studie ergab drei zentrale Erkenntnisse:

› **Sicherheitsteams müssen Mitarbeiter ohne Büroarbeitsplatz betreuen und schützen.** Auf der einen Seite haben Büroangestellte geringere Sicherheitsanforderungen und sind weniger Risiken ausgesetzt, da sie durch den Standort oder das Büro, in dem sie sich befinden, geschützt sind. Auf der anderen Seite werden Mitarbeiter ohne Büroarbeitsplatz und Wissensarbeiter eher vernachlässigt. Firmen müssen sich auch ihnen widmen und erkennen, dass ein Universalansatz einfach nicht für jeden Mitarbeiter funktioniert.

› **Information Worker umgehen die Sicherheit nicht aus Bösartigkeit, sondern um produktiv arbeiten zu können.** Die heutige digitale Umgebung erfordert von den Mitarbeitern schnelles Handeln. Offensichtlich hilft ihnen die Sicherheit dabei nicht, vor allem wenn sie außerhalb des Unternehmens arbeiten. Um zu bekommen, was sie benötigen, um ihre Kunden besser bedienen zu können, umgehen sie Sicherheitsrichtlinien.

› **Mitarbeitergewohnheiten verstärken schlechte Sicherheitspraktiken.** Unterschiedliche Persönlichkeitstypen arbeiten in der Art und Weise, die ihre Rolle entspricht. Zum Beispiel müssen Mitarbeiter ohne Büroarbeitsplatz sowie Wissensarbeiter Daten mit Kollegen und Dritten teilen, aber ein USB-Stick oder eine CD kann verloren gehen. Mit anderen Worten: Das Risiko besteht in dem unsicheren Gerät, und Arbeitsgewohnheiten verstärken es.

METHODIK

Dieses Technology Adoption Profile wurde von Dell in Auftrag gegeben. Die individuellen Fragen wurden 400 Information Workern aus allen Branchen in Australien, Indien, Großbritannien und den USA vorgelegt.

Die individuelle Umfrage wurde im Zeitraum Juli bis Oktober 2017 durchgeführt. Weitere Informationen zum Daten-Panel von Forrester und dessen Consulting-Dienstleistungen für die Technologiebranche finden Sie unter Forrester.com.

Projektleiter:

Tarun Avasthy
Market Impact Consultant