Future of Work mit EPM, Identitäts- und Zugriffs-kontrollen ermöglichen

Januar 2022

Autoren:

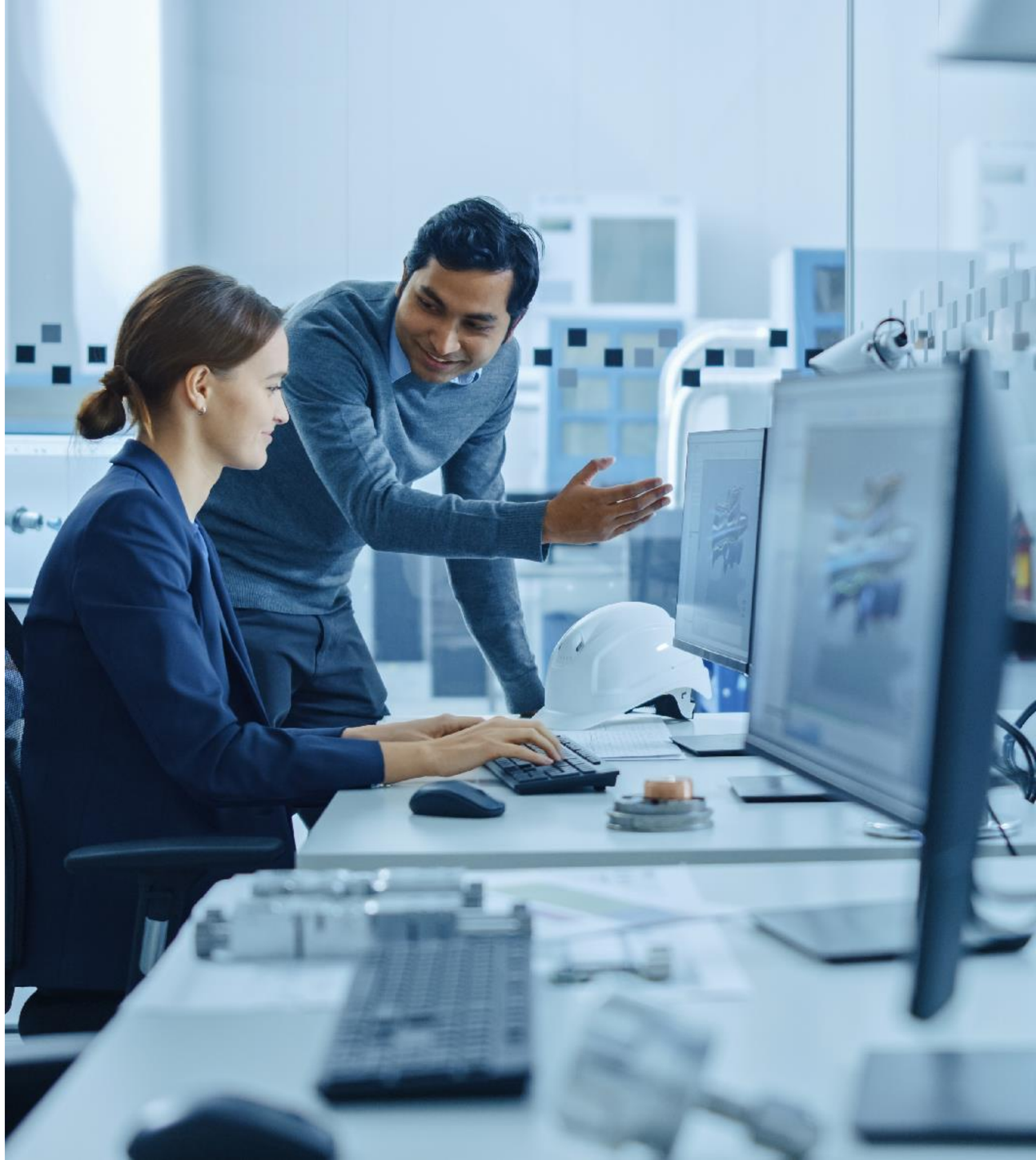
Mark Child
Research Manager, European Security, IDC

Jay Bretzmann
Program Director, Security Products, IDC

IDC #EUR148370521

Ein IDC InfoBrief, gesponsert von

LastPass



Unruhige Gewässer

- Die COVID-19-Pandemie stellt eine der größten Herausforderungen aller Zeiten für Unternehmen dar, die wir vermutlich auch noch nicht überstanden haben.
- Es besteht jedoch Hoffnung. Impfstoffe und innovative Schutzmaßnahmen erlauben eine Rückkehr zu einer gewissen Normalität, und Unternehmen, Handel und Reisen nehmen wieder Fahrt auf.

EINE UNGLEICHMÄßIGE ERHOLUNG

Nach Angaben der Weltorganisation für Tourismus UNWTO stieg die Zahl der nach Europa einreisenden Touristen von Dezember 2020 bis Mai 2021 um 75 Prozent. In Nord- und Südamerika stieg sie jedoch nur um 14 Prozent und in Asien/Pazifik um 8,5 Prozent. In Afrika ging sie um 35 Prozent zurück.

PROBLEME IN DEN LIEFERKETTEN VERZÖGERN DIE ERHOLUNG

Laut The Economist hat der europäische Einzelhandel mit höheren Fracht- und Arbeitskosten sowie Unterbrechungen der Lieferketten zu kämpfen, was sich auf den Umsatz auswirkt. In den USA haben FedEx, UPS, Walmart und zwei große Häfen auf Arbeitszeiten rund um die Uhr (24/7) umgestellt, um Engpässe in der Lieferkette zu beheben, so die Financial Times*.

CHIP-KRISE TRIFFT DEN HEIMISCHEN MARKT

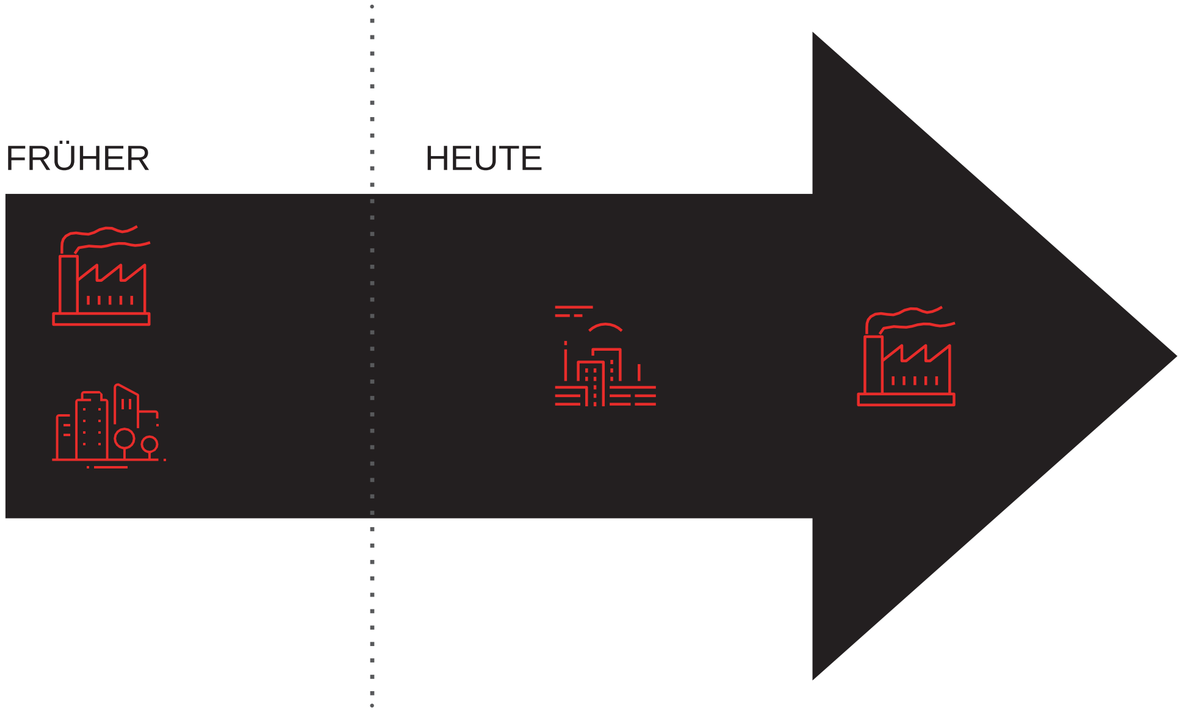
Die Halbleiterknappheit wird dazu führen, dass die weltweite Fahrzeugproduktion im Jahr 2021 um bis zu 5 Millionen Einheiten sinken wird, so das Beratungsunternehmen AlixPartners**. Apple erwartet für das vierte Quartal des Geschäftsjahrs einen Rückgang von bis zu 6 Milliarden US-Dollar, während Samsung meldet, dass sich möglicherweise die Einführung seiner neuesten Version des Smartphones Galaxy Note verzögern wird.

AUSWIRKUNGEN AUF DAS BUDGET

30 Prozent der Unternehmen weltweit gaben an, dass aufgrund von COVID-19 die Sicherheitsbudgets für 2021 reduziert wurden***. Noch höher ist der Wert in Frankreich (41 Prozent), Singapur (38 Prozent) und dem Vereinigten Königreich und Irland (37 Prozent).

*Quelle: https://www.ft.com/content/8055d806-3166-48c9-9786-9bdea0e2d806
**Quelle: https://www.washingtonpost.com/technology/2021/03/01/semiconductor-shortage-halts-auto-factories/
***Quelle: IDC/LastPass Customer-Umfrage, 2021 (n = 700)

Die Zeiten, in denen Mitarbeiter an einen Büroarbeitsplatz gebunden sind, sind vorbei



FUTURE-OF-WORK-ANFORDERUNGEN

- Arbeiten von überall aus
- Hybride Arbeitsmodelle
- Flexibilität
- Frei verfügbare Arbeitsplätze
- Nutzererfahrungen (UX)
- Produktivität
- Mobilität
- Unsichtbare Sicherheit
- B2E-, B2P- und B2C-Identitätsmanagement

Nur sehr wenige Unternehmen planen eine Rückkehr zu alten Arbeitsnormen. Die Denkweisen haben sich von der Arbeit im Büro zur Arbeit von zu Hause und von überall aus verlagert, von traditionellen Büros und Bürokomplexen zu hybriden und frei verfügbaren Arbeitsplätzen.

Die Arbeitgeber haben erkannt, dass ihre Arbeitskräfte aus der Ferne und dennoch produktiv arbeiten können. Sie haben neue Möglichkeiten kennengelernt und möchten diese für sich nutzen. **Doch die Herausforderungen in Bezug auf Zusammenarbeit und Sicherheit verbleiben**.

Laut einer gemeinsamen Umfrage von IDC und LastPass strebt **eines von drei Unternehmen weltweit** angesichts der durch COVID-19 verursachten Betriebseinschränkungen ein Gleichgewicht zwischen Nutzererfahrung, Produktivität und Sicherheit an.

Identitäts- und Zugriffskontrollen sind Kernkomponenten für die Bewältigung vieler Anforderungen an die Zukunft der Arbeit.

Identitätsverletzungen passieren viel zu häufig

Von Unternehmen, die nach einer Netzwerksicherheitsverletzung unter Datenverlust litten, gaben

83 Prozent

an, die Verletzung sei das Ergebnis einer Identitätsverletzung wie **Phishing**

In Deutschland liegt dieser Anteil bei **82 Prozent**, in den USA beträgt er **87 Prozent**, in Indien **90 Prozent**.

„Gleichgewicht zwischen Sicherheitsanforderungen und Nutzererfahrung für Mitarbeiter“ ist die

größte

Identitätsherausforderung (38 Prozent), gefolgt von **„Mitarbeiter, die mit zu vielen Passwörtern zu kämpfen haben“** (32 Prozent)

„Zu viele Passwörter“ ist eine wesentliche Herausforderung für **36 Prozent** der großen Unternehmen und **für 40 Prozent** der Organisationen des öffentlichen Sektors.

45 Prozent

der Unternehmen haben eine **Lösung für die Verwaltung von Passwörtern im Unternehmen** bereitgestellt, um diese Herausforderungen zu bewältigen.

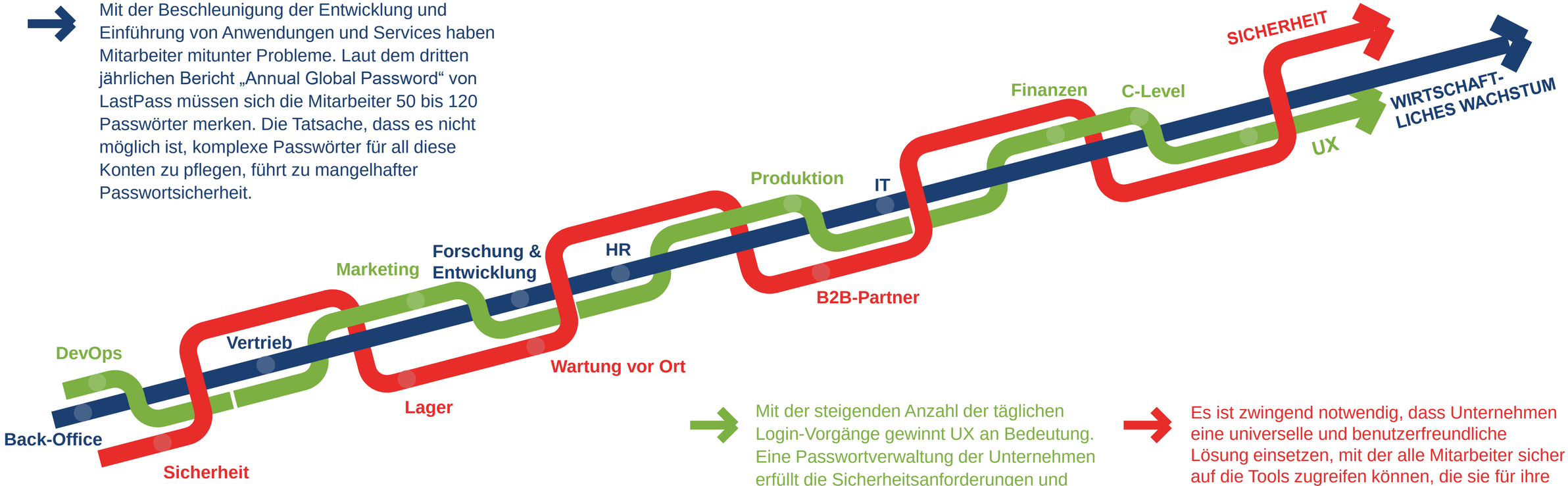
Dazu gehören sowohl **große Unternehmen**, die eine zusätzliche Schutzebene und Benutzerfreundlichkeit bieten möchten, als auch **kleine und mittlere Unternehmen** mit begrenzten Sicherheitsbudgets.

In Asien/Pazifik **(52 Prozent)** ist die EPM-Verbreitung noch höher und in vertikalen Märkten wie dem verarbeitenden Gewerbe **(60 Prozent)** und dem Einzelhandel **(50 Prozent)** ist sie am höchsten.

Quelle: IDC/LastPass Customer-Umfrage, 2021 (n = 700)

Beschleunigte Geschäftsentwicklungen erfordern allgegenwärtige Sicherheit … und Nutzerfreundlichkeit

Mit der Beschleunigung der Entwicklung und Einführung von Anwendungen und Services haben Mitarbeiter mitunter Probleme. Laut dem dritten jährlichen Bericht „Annual Global Password“ von LastPass müssen sich die Mitarbeiter 50 bis 120 Passwörter merken. Die Tatsache, dass es nicht möglich ist, komplexe Passwörter für all diese Konten zu pflegen, führt zu mangelhafter Passwortsicherheit.



Mit der steigenden Anzahl der täglichen Login-Vorgänge gewinnt UX an Bedeutung. Eine Passwortverwaltung der Unternehmen erfüllt die Sicherheitsanforderungen und gewährleistet gleichzeitig eine einheitliche und komfortable Nutzererfahrung.

Es ist zwingend notwendig, dass Unternehmen eine universelle und benutzerfreundliche Lösung einsetzen, mit der alle Mitarbeiter sicher auf die Tools zugreifen können, die sie für ihre Aufgaben benötigen. **Sicherheitskontrolle müssen für alle Benutzer transparent und zu bewältigen sein.**

Dem Gegner entgegentreten

Sind Cyberkriminelle einfach zu gut in dem, was sie tun?

- Laut einer IDC-Studie setzen 60 Prozent der europäischen Unternehmen Digital-First-Strategien um oder bauen diese aus, um geschäftliche Ergebnisse zu erzielen. Die Nutzung neuer Partner und Lieferanten bringt geschäftliche Vorteile, erhöht aber die Anfälligkeit.
- Wie können Unternehmen einem Lieferanten sicheren Zugriff auf die erforderlichen Systeme gewähren, ohne sich potenziell einer Gefährdung auszusetzen? Passwörter und Authentifizierung können Schwachstellen sein, wenn diese Mechanismen nicht geschützt sind.
- Darüber hinaus werden unsere Unternehmen weiterhin durch Ransomware-Angriffe und Angriffe auf die Lieferkette bedroht. Das Risiko für die Lieferkette wird sich weiter erhöhen, wenn wir die Pandemie hinter uns lassen und die Globalisierung sich beschleunigt.

Nach Angaben im Bericht 2021 zur Datenschutzverletzung von Verizon erfolgen ...

... 93 Prozent der Angriffe von finanziell motivierten Akteuren des organisierten Verbrechens. Am häufigsten werden Anmeldedaten kompromittiert (44 %), wobei Bedrohungsakteure zu 57 Prozent extern und zu 44 Prozent intern auftreten (häufig gibt es mehrere Akteure).

Die Verletzungsmuster für kleine Unternehmen (< 1.000 Mitarbeiter) entsprechen denen für große Unternehmen, wobei etwa jedes vierte eine Offenlegung von Daten betrifft. Es gilt jedoch zu beachten, dass große Unternehmen in der Regel Sicherheitsverletzungen schneller (innerhalb von Stunden/Tagen) erkennen können als kleine Unternehmen.

Im Jahr 2020 waren die Login-Daten von über 500.000 Spielerkonten beim US-Videospielhersteller Activision Ziel eines Angriffs zum Diebstahl von Anmeldedaten, die online veröffentlicht wurden und Hackern Zugang zu den Konten bei Call of Duty boten.

Laut dem Bericht „Psychologie von Passwörtern“ 2021 von LastPass verwenden 65 Prozent der Nutzer immer oder meistens dasselbe Passwort oder eine Variation davon, und 45 Prozent haben ihr Passwort auch nach einer Sicherheitsverletzung nicht geändert. Dieses Verhalten führt zu einer höheren Anzahl von Verletzungen, wodurch Unternehmen und Verbraucher einem höheren Risiko ausgesetzt sind.

Angriffe erstrecken sich über alle Regionen und Branchen

Nintendo – Gaming

- Japan
- 2020
- Diebstahl von Anmeldedaten
- Ein Angriff auf Zugangsdaten, bei dem zuvor offengelegte Benutzer-IDs und Passwörter des Videospielunternehmens Nintendo verwendet wurden, gab Hackern Zugriff auf über 300.000 Spielerkonten.

HSBC – Bankwesen

- Vereinigtes Königreich
- 2018
- Diebstahl von Anmeldedaten
- Bei schätzungsweise 14.000 Kunden wurden Namen, Adressen, Telefonnummern, E-Mail-Adressen, Geburtsdaten, Kontonummern, Kontostände und Transaktionsverläufe offengelegt.

UniCredit – Bankwesen

- Italien
- 2019
- E-Mail-Phishing
- Bei einem Sicherheitsvorfall wurden 3 Millionen Kundendatensätze, darunter Kundennamen, Wohnorte, Telefonnummern und E-Mails, geleakt.

EyeMed, Aetna – Gesundheitswesen

- USA
- 2020
- E-Mail-Phishing
- Ein Phishing-Angriff auf EyeMed enthüllte die personenbezogenen und medizinischen Informationen von 484.000 Aetna-Mitgliedern, 60.500 Mitgliedern des Tufts-Gesundheitsplans und 1.300 Mitgliedern des Blue Cross Blue Shield.

HSE.ie – Gesundheitswesen

- Irland
- 2021
- Conti-Ransomware
- Die landesweite Abschaltung des IT-Systems hatte Auswirkungen auf Krankenhäuser im ganzen Land, verhinderte den Zugriff auf elektronische Aufzeichnungen, sorgte dafür, dass Radiologiesysteme abgeschaltet wurden und zwang zu Terminabsagen. Patientendaten wurden online veröffentlicht. Die geschätzten Kosten des Angriffs lagen bei über 100 Millionen EUR.

Verschiedene bekannte Personen

- Deutschland
- 2018
- Ein einziger Hacker hat private Daten von fast 1.000 deutschen Politikern und Prominenten enthüllt. Die Ermittler berichteten, dass die meisten der gehackten Konten einfache Passwörter wie „ILoveYou“ oder „1,2,3“ hatten, was es dem Hacker relativ einfach machte, Zugang zu E-Mail-Konten, Cloud-Diensten und sozialen Netzwerken zu erhalten.

Wie können Sicherheitslösungen das Problem bewältigen?

Wo sich Identitätskontrollen und Risikomanagement überschneiden

Verizon hat zudem die Ergebnisse seines Berichts zur Datenschutzverletzung mit den vom Center for Internet Security (CIS) empfohlenen Kontrollen verglichen. Die wichtigsten Kontrollen, die jedes Unternehmen unabhängig von Größe und Budget durchführen sollte, umfassen **Account-Management, Zugriffskontrolle sowie Schulungen zu Sicherheitsbewusstsein und -fähigkeiten.**

Zu den wichtigsten Fragen gehören:

Welche Tools stehen zur sicheren Authentifizierung und Gewährleistung eines sicheren und angemessenen Zugriffs für Remote-Mitarbeiter zur Verfügung?

Wie können Unternehmen die anhaltenden Probleme schwacher Passwörter und schlechter Passwortsicherheit bewältigen, die der beste Freund eines Hackers sind?

Welche Sicherheitsvorkehrungen können getroffen werden, um zu verhindern, dass große Bedrohungen wie z. B. Ransomware in das Unternehmen eindringen und sich ausbreiten?

Konzepte wie die Authentifizierung ohne Passwort und die Zero-Trust-Zugriffskontrolle werden als Allheilmittel für alle angeboten, aber um diese Ziele zu erreichen, sind mehrere Komponenten und eine umfassende Strategie erforderlich. Es gibt keine sofort einsatzbare Lösung, die über Nacht Zero-Trust-Lösungen einführt.

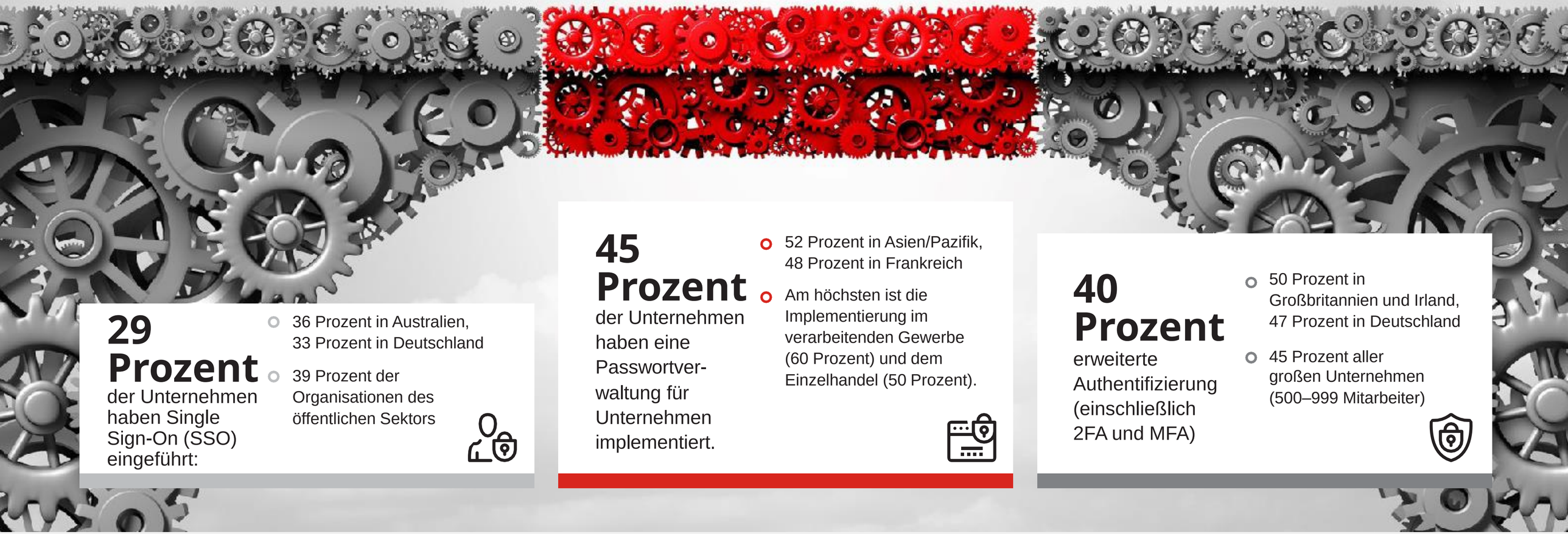
Welche Schritte können Unternehmen gehen, um damit zu beginnen, ihr Risiko durch Identitäts- und Zugriffskontrollen zu verringern?

Überwindung von Infrastruktur- und Prozesslücken mit einer einzigen Bereitstellung ist nicht immer möglich

- Jedes Unternehmen möchte einen Schritt voraus sein, wenn es eine Marktchance erkennt.
- Entwicklungsteams werden durch Nachrichten über schnelle Markteinführungen, den schnellen Ausfall jetzt oder in der Zukunft aufgeschreckt.
- Unternehmen wollen so schnell wie möglich expandieren.

- Verzögerungen beim Mitarbeiterzugriff und die völlige Unfähigkeit, Anwendungen zur Unterstützung von Produktivität und Geschäftszielen zu verwenden, sollten nicht auftreten, da SAML (SSO) nicht unterstützt wird.
- B2C-Lösungen müssen die vielleicht unbeständigste Gruppe an Interessenten und Kunden ansprechen, bei denen die Konkurrenz nur einen Klick entfernt ist.
- Für viele Unternehmen ist eine Kombination aus Sicherheitstools zur Erfüllung der Identitätsanforderungen aller Benutzer erforderlich.

Bereitstellung von Lösungen zur Überbrückung der Lücken



29 Prozent der Unternehmen haben Single Sign-On (SSO) eingeführt:

- 36 Prozent in Australien, 33 Prozent in Deutschland
- 39 Prozent der Organisationen des öffentlichen Sektors

45 Prozent der Unternehmen haben eine Passwortver-waltung für Unternehmen implementiert.

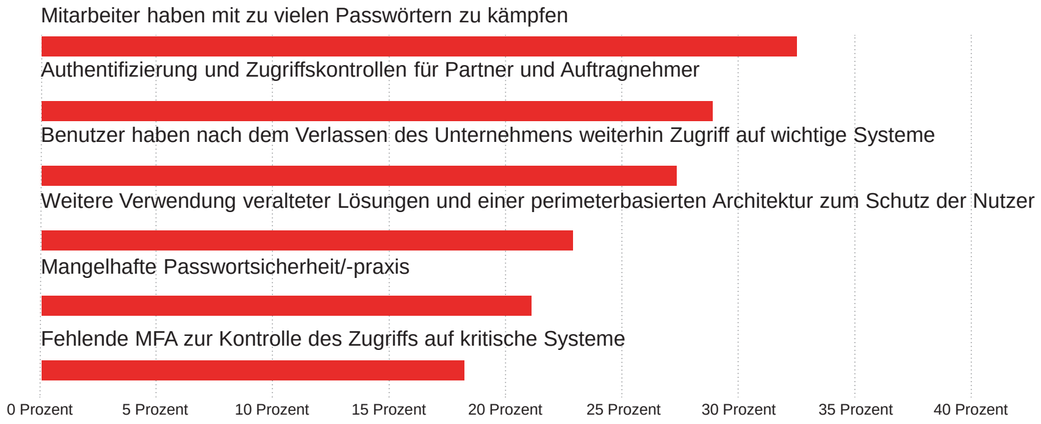
- 52 Prozent in Asien/Pazifik, 48 Prozent in Frankreich
- Am höchsten ist die Implementierung im verarbeitenden Gewerbe (60 Prozent) und dem Einzelhandel (50 Prozent).

40 Prozent erweiterte Authentifizierung (einschließlich 2FA und MFA)

- 50 Prozent in Großbritannien und Irland, 47 Prozent in Deutschland
- 45 Prozent aller großen Unternehmen (500–999 Mitarbeiter)

Unternehmen kämpfen weiterhin mit grundlegenden Identitäts- und Zugriffskontrollen …

Welchen der folgenden Herausforderungen sieht sich Ihr Unternehmen in Bezug auf Identität und Zugriff gegenüber?



… wie zum Beispiel der Aufhebung des Zugriffs der Nutzer, wenn sie das Unternehmen verlassen.

Unternehmen sind nach wie vor stark von älteren Lösungen und einer perimeterbasierten Architektur **abhängig und sind aufgrund mangelnder Passwortsicherheit unnötigen Risiken** ausgesetzt.

Im Identitäts- und Zugriffsbereich bestehen erhebliche Verbesserungsmöglichkeiten.

- 42 Prozent der australischen Unternehmen haben Schwierigkeiten, Sicherheit und Nutzererfahrung für ihre Mitarbeiter in Einklang zu bringen.
- 32 Prozent der französischen Unternehmen sehen in Authentifizierung und Zugriffskontrollen für Partner und Auftragnehmer eine Herausforderung.

- 43 Prozent der großen Unternehmen (500–999 Mitarbeiter) haben Schwierigkeiten, ein Gleichgewicht zwischen Sicherheit und Nutzererfahrung für die Mitarbeiter zu finden.
- **32 Prozent der kleinen Unternehmen (10–99 Mitarbeiter) geben an, dass ihre Mitarbeiter mit zu vielen Passwörtern zu kämpfen haben.**

- 33 Prozent der Dienstleistungsunternehmen haben Probleme damit, den Systemzugang von Nutzern nach Ausscheiden aus dem Unternehmen zu löschen.
- 42 Prozent der Transportunternehmen geben an, dass ihre Mitarbeiter Schwierigkeiten mit zu vielen Passwörtern haben.

Quelle: IDC/LastPass Customer-Umfrage, 2021 (n = 700)

Die EPM-Einführung ist durch mehrere Treiber und Konfigurationen gekennzeichnet

EPM als alleinige Lösung:

45 Prozent geben an, komplexere Identitätslösungen wie SSO und MFA zu begrüßen, doch sie haben nicht das nötige Budget (dies gilt für 55 Prozent in Asien/Pazifik und 48 Prozent in Nordamerika).

34 Prozent geben an, komplexe Lösungen wie SSO und MFA zu begrüßen, **aber sie verfügen nicht über die Ressourcen, sie bereitzustellen und auszuführen** (dies gilt für 41 Prozent der europäischen Unternehmen).

27 Prozent geben an, dass ihr Unternehmen zu klein ist, um Lösungen wie SSO und MFA zu benötigen.

EPM in Kombination mit SSO, aber ohne MFA:

48 Prozent geben an, dass SSO die Passwortmüdigkeit verringert, aber einige wenige Anwendungen erfordern zusätzliche MFA-Kontrollen, die die Müdigkeit überwinden würden.

46 Prozent geben an, **dass Passwortmamangement zusätzlichen Schutz in Bezug auf die Schatten-IT-Nutzung bietet.**

40 Prozent geben an, dass SSO nicht universell für alle Apps, die sie nutzen wollen, einsetzbar ist, weshalb sie auch ein Passwortmanagement benötigen.

EPM in Kombination mit SSO und MFA:

91 Prozent geben an, dass EPM eine Benutzerfreundlichkeit bietet, die Mitarbeiter bei **häufig besuchten externen Websites** zu schätzen wissen.

77 Prozent geben an, **dass es besser ist, je mehr Ebenen der Kontrolle und des Schutzes vorhanden sind, desto besser**...

75 Prozent geben an, dass SSO nicht universell für alle Appes, die sie nutzen, einsetzbar ist, weshalb sie auch ein Passwortmanagement benötigen.

Eine Lösung für alle im Raum

Ein optimales Identitäts- und Zugriffsverwaltungstool sollte:

- In jedem Team eingesetzt und effektiv sein
- Sich wie ein Sicherheitstool verhalten, aber nicht wie eines aussehen
- Benutzerfreundlich für alle sein, von Mitarbeitern mit hoher IT-Kompetenz bis zu solchen, die eher eine IT-Phobie haben

Zu den Funktionen eines idealen Tools gehören:

- Einfache Bereitstellung und Integration mit allen wichtigen Anwendungen, die Ihr Unternehmen einsetzt
- Benutzertransparenz und ein reibungsloses Erlebnis
- Kosten, die für den Mittelstand und Unternehmen zu bestreiten sind

Die Passwortverwaltung in Unternehmen bietet:

- Einen **sicheren Aufbewahrungsort für jeden Login jedes Mitarbeiters, auf den niemand sonst** zugreifen kann, nicht einmal Administratoren oder LastPass selbst
- Zusätzliche Sicherheitskontrollen, z. B. die Überprüfung der Authentizität einer Website vor der Eingabe von Anmeldeinformationen
- Mehrwert wie zusätzliche Konten für Familienmitglieder, wenn Mitarbeiter aus dem Homeoffice tätig sind

Über LastPass

LastPass

Verbinden Sie Mitarbeiter einfach und sicher mit ihren Aufgaben.

Die IT steht vor der Herausforderung, das Unternehmen zu schützen, ohne die Produktivität zu beeinträchtigen.

Von der Authentifizierung bis zum Zugriff auf Passwörter verwaltet LastPass jeden Einstiegspunkt in Ihr Unternehmen, sodass Sie Risiken minimieren und gleichzeitig die Produktivität Ihrer Mitarbeiter steigern können.

Umfassende Sicherheits-kontrollen

Sofort einsatzbereite Integrationen

Adaptive Authentifizierung

Einfache Benutzerver-waltung und Berichterstellung

Praktische Passwortfreigabe

Reibungslose Nutzererfahrung

Dark-Web-Überwachung

Entwickelt für Sicherheit als oberste Priorität

Nahtlose Bereitstellung, Verwaltung und Erfahrung

Über 85.000 Unternehmen nutzen LastPass

Über 30 Mio. Benutzer

Ein kostenloses Familienkonto für Mitarbeiter

Über IDC

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informations- und Verbrauchertechnologie und der Telekommunikation. IDC analysiert und prognostiziert technologische und branchenbezogene Trends und Potenziale und ermöglicht seinen Kunden so eine fundierte Planung ihrer Geschäftsstrategien sowie ihres IT-Einkaufs. Mehr als 1.100 IDC Analysten in über 110 Ländern vermitteln globale, regionale und lokale Erkenntnisse zu technologie- und branchenbezogenen Geschäftschancen und Trends. Seit über 50 Jahren vertrauen Entscheidungsträger und IT-Führungskräfte bei der Entscheidungsfindung auf IDC. IDC ist ein Tochterunternehmen von IDG, dem weltweit führenden Technologiemedien-, Research- und Veranstaltungsunternehmen.

IDC UK
5th Floor, Ealing
Cross, 85 Uxbridge
Road London
W5 5TH, Großbritannien
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Unternehmenszentrale
140 Kendrick Street,
Building B, Needham,
MA 02494 USA
+1 508 872 8200
www.idc.com