WALLIX
CYBERSECURITY SIMPLIFIED

Cybersecurity meets Zeitgeist

Cybersecurity meets Zeitgeist

TABLE OF CONTENTS

WALLIX
CYBERSECURITY SIMPLIFIED


IT-Sicherheit muss
mit dem Zeitgeist
gehen.

IT-SICHERHEIT MUSS MIT DEM ZEITGEIST GEHEN – WAS DAS BEDEUTET UND WIE DEN AKTUELLEN HERAUSFORDERUNGEN BEGEGNET WERDEN KANN

Wir haben Revolution! Mal wieder. Gemeint sind jene epochalen Umbrüche, von denen die Menschheit bereits einige hinter sich hat. Nehmen wir beispielsweise die Neolithische Revolution: Der Mensch wurde sesshaft, lernte Ackerbau und Viehzucht sowie Vorratshaltung. Mit der Lebensweise als reine Jäger und Sammler war es ein für alle Mal vorbei. Näher an unserer Zeit ist die Industrielle Revolution mit nicht minder weitgreifenden Auswirkungen auf die Gesellschaft als Ganzes und vor allem auf das Arbeitsleben. Die radikalen Veränderungen der gewerblichen Produktionsformen hatten eine zunehmende Urbanisierung und die Ausbildung des Proletariats zur Folge. Aktuell ist eine weitere, umwälzende Revolution im Gange:
die Digitale Revolution.

Wir erleben gerade sehr eindrücklich, wie sich unsere Arbeitswelt ein weiteres Mal eklatant verändert und gesellschaftliche Paradigmen verschieben. Wollte man all das, was sich da aktuell bewegt und entwickelt, die Denk- und Fühlweisen eines ganzen Zeitalters in einem Wort zusammenfassen, so landet man bei „Zeitgeist"!

Dieser Ausdruck versucht nicht mehr und nicht weniger, als die kennzeichnende Eigenart einer bestimmten Epoche einzufangen. Das deutsche Wort Zeitgeist ist übrigens ein wahrer Exportschlager und hat sich über das Englische als Lehnwort in zahlreichen anderen Sprachen etabliert. So kennt man im Englischen beispielsweise das Adjektiv zeitgeisty. Der geneigte Leser fragt sich möglicherweise, wie man ein eher trockenes Thema wie IT-Security mit dem
Zeitgeist zusammen bringt?

Im Grunde ist es denkbar einfach: „Alles hängt mit allem zusammen" – diese elementare Erkenntnis geht auf Alexander von Humboldt zurück, der in seinen Werken die Ansicht vertrat, dass unsere Umwelt nur im Zusammenspiel mit dem menschlichen Wirken zu betrachten sei. Humboldt bezog sich auf das zu seinen Lebzeiten vorherrschende Naturverständnis, und keineswegs auf die Technologie, die doch heute so bestimmend für unser Leben ist. Trotzdem ist sein Satz gültig. So wird niemand bestreiten, dass die COVID-19 Pandemie beziehungsweise die Maßnahmen, die zu ihrer Eindämmung ergriffen wurden und werden, zahlreiche Auswirkungen auf die Gesellschaft als Ganzes, die Art und Weise, wie wir arbeiten, und damit einhergehend wiederum auf die Anforderungen im Bereich der IT Sicherheit in den Unternehmen haben.

ALLES HÄNGT ZUSAMMEN!

Dabei sind die Veränderungen, die sich momentan in der modernen Arbeitswelt vollziehen, beileibe keine Prozesse, die durch diese Pandemie erst ausgelöst wurden. Die vielzitierte Digitale Transformation, das sich zunehmender Beliebtheit erfreuende Konzept des New Work, der Trend zum Home Office – all diese Entwicklungen waren schon längst im Gange und erfuhren durch die Corona-Krise lediglich einen neuen Spin.

Dazu kommt, dass viele dieser Themen vor dem Hintergrund des erzwungenen Social Distancing einfach nur neu bewertet werden: Mancher eingefleischte Home Office-Skeptiker beispielsweise sieht sich nach den Wochen der praktischen Erfahrung mit dieser Arbeitsweise eines Besseren belehrt. Wie in vielen anderen Bereichen auch werden diese neu gewonnenen Einsichten langfristig in ganz neuen Gewohnheiten, Verhaltensänderungen und vor allem in der Arbeitswelt in neuen Prozessen und Konzepten münden. Das hat natürlich Auswirkungen auf die IT Sicherheit.

DIE REICHHALTIGE LANDSCHAFT DER BEDROHUNGEN

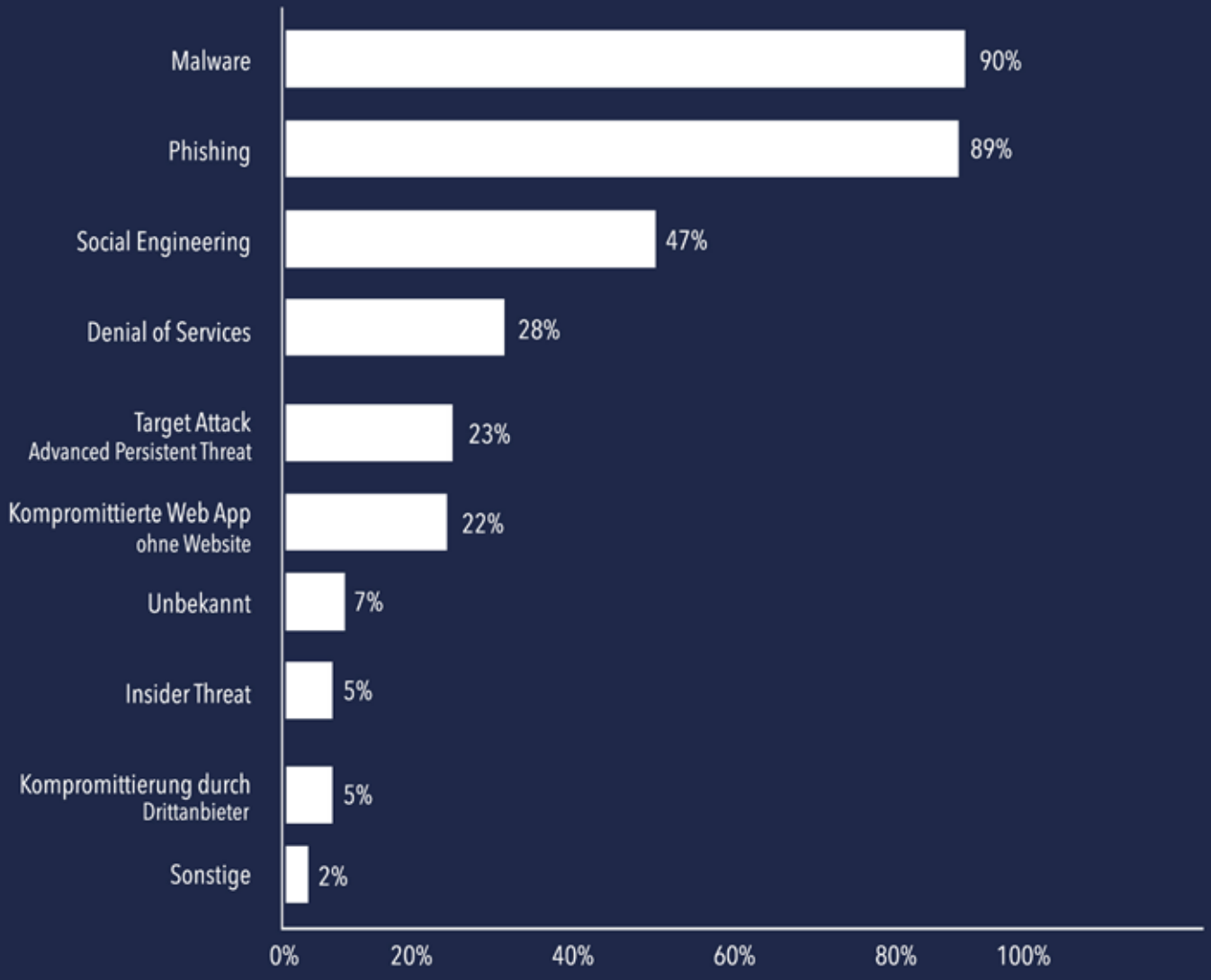
Bedrohungen für eine moderne IT-Landschaft ergeben sich natürlich nicht nur aus den Verwerfungen durch die Corona-Krise. Weitere Treiber einer zusehends komplexer werdenden Bedrohungslage sind auch langfristig wirkende Entwicklungen wie die zunehmende Anbindung von Partnern und Kunden im Zuge der digitalen Transformation oder die Vernetzung von OT und IT als Folge der Industrie 4.0. Auch Trends wie BYOD (Bring Your Own Device) schaffen immer neue Herausforderungen für die IT-Security-Teams in den Unternehmen.

Dazu trägt auch die fortschreitende Globalisierung ihr Scherflein bei. Sie führt dazu, dass Organisationen extrem flexibel sein müssen, um sich im immer härter werdenden Wettbewerb zu behaupten. Wer als Unternehmen den gestiegenen Erwartungen der Kunden, aber auch der Partner gerecht werden will, muss sich öffnen. Die Zusammenarbeit mit externen Dienstleistern bringt den Organisationen durchaus handfeste Vorteile. So lassen sich auf diese Weise die Kosten und Tätigkeiten über verschiedene geografische Gebiete hinweg deutlich optimieren; daher ist dieses Konzept aus gutem Grund weit verbreitet.

Öffnung aber bedeutet, Fernzugriffe auf die unternehmenseigene IT Infrastruktur zuzulassen.

Das führt in vielen Fällen zu einer ganzen Reihe von teilweise nicht einmal dokumentierten privilegierten Zugriffsrechten auf die Ressourcen des Unternehmens. Anders ausgedrückt: Geschäftspartner können problemlos auf sensible oder sogar kritische Inhalte zugreifen. Genau das macht diese Zugänge auch so überaus attraktiv für Cyberkriminelle, die sie mit Vorliebe als Einfallstor nutzen. Aus diesem Grund müssen die Unternehmen die Zugriffe der verschiedenen Dienstleister auf interne strategische und kritische Ressourcen unbedingt unter Kontrolle haben. Und die Maßnahmen zum Schutz dieser wertvollen Assets müssen auch nachvollziehbar sein. Allein schon deswegen, um einer ganzen Batterie von Vorschriften zu genügen, deren Nichteinhaltung teilweise empfindliche Geldstrafen nach sich ziehen kann (DSGVO, NIS, LPM, PCI-DSS etc.).

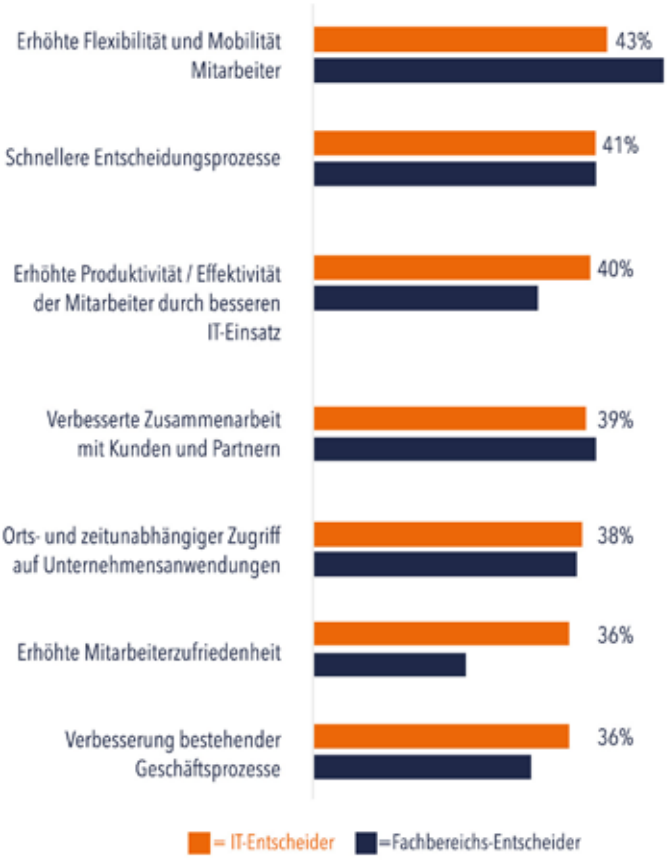
Welche Arten von Cyberangriffen haben Sie in Ihrem Unternehmen identifiziert?



Quelle: KPMG Statista 2019

KOMPROMITTIERTE ENDGERÄTE

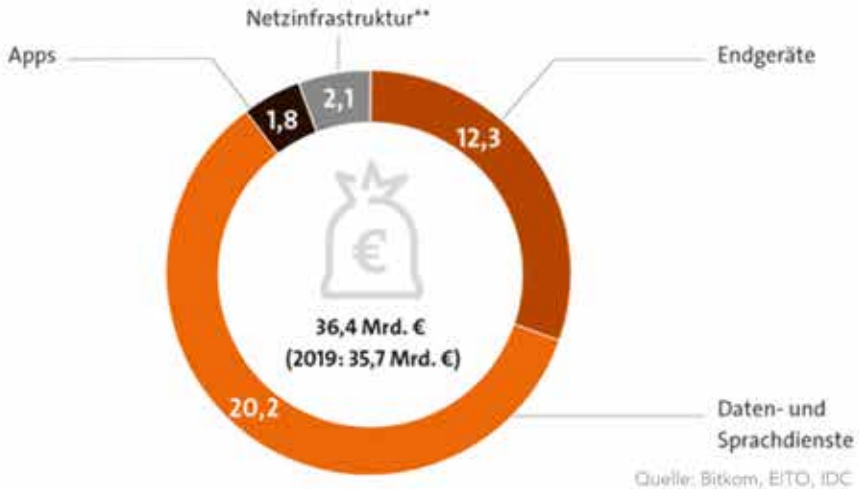
Nicht immer sind es Außenstehende, die durch ihre Zugänge zur IT Infrastruktur ein gehöriges Gefahrenpotenzial erzeugen. Nicht nur seit sie es aufgrund von COVID-19 zwangsweise praktizieren müssen, auch ganz generell finden mehr und mehr Menschen Geschmack am unabhängigen Leben als „digitaler Nomande", der eben nicht nur von zuhause aus, sondern von überall aus und zu jeder Zeit auf die Datenserver des Arbeitgebers zugreift. Der Einsatz von Mobilsystemen hat zudem auch aus Arbeitgebersicht eine ganze Reihe von Vorteilen, die auf wichtige Themen wie Produktivität und Mitarbeiterzufriedenheit einzahlen. Im Zuge dessen erfreuen sich mobile Endgeräte zunehmender Beliebtheit – und bedeuten für die Security-Teams immer weitere Einfallstore für Cyberattacken.



Quelle: Einer Studie von IDC Deutschland zufolge erwarten sich deutsche Unternehmen vom Einsatz von Mobilsystemen handfeste wirtschaftliche Vorteile.

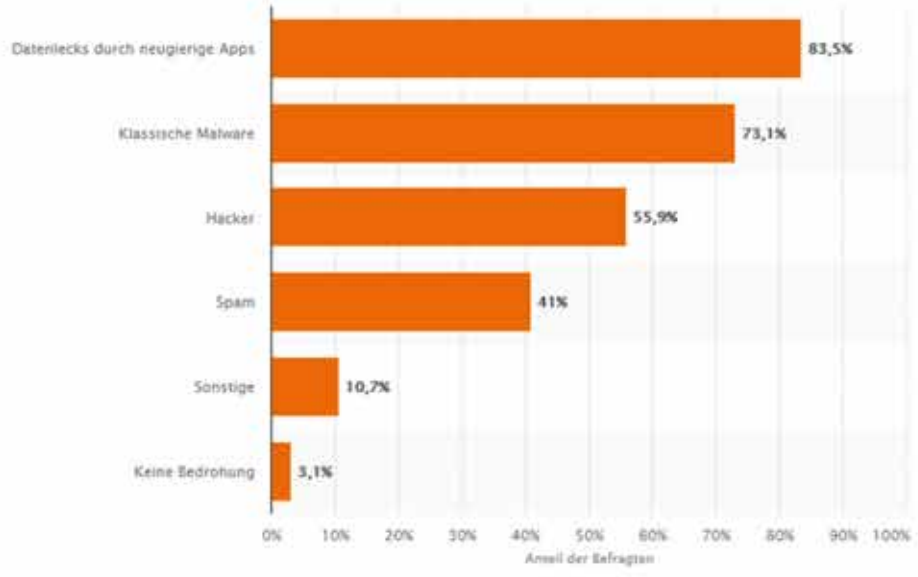
Markt rund ums Smartphone wächst um 2%

Umsätze im Smartphone-Ökosystem in Deutschland 2020* (in Mrd. Euro)



Quelle: Bitkom, EITO, IDC

Sicherheitsrisiken bei der Nutzung mobiler Endgeräte



Quelle: Statista

Wie bereits weiter oben ausgeführt, wird der Trend zur Nutzung mobiler Devices durch die Bekämpfungsmaßnahmen von COVID-19 eher noch verstärkt. Für die Unternehmen bedeutet dies unter dem Strich einen weiteren Baustein der wachsenden Komplexität, mit der sie sich nicht nur in Bezug auf ihre IT Security Strategien auseinander setzen müssen. Ein Aspekt dieses immer umfassenderen Themas sind eben die Gefahren, die von solchen Endpoints ausgehen.

Da der Zugriff auf die IT Infrastruktur mittels mobiler Endgeräte in Zukunft also absehbar eher noch deutlich zunehmen wird, ist eine kritische Überprüfung der etablierten Security-Strategie das Gebot der Stunde. Die Lösung kann nur lauten, die Komplexität der IT Security Infrastruktur auf ein absolut notwendiges Level zu reduzieren, getreu dem Motto, „Weniger ist mehr". Das bedeutet in der Praxis „So wenig Rechte wie möglich, soviel technischer Endpoint-Schutz wie nötig".

Lösungen für die Verwaltung von Applikations- und Benutzerprivilegien auf den entsprechenden Endpoints sind ein höchst wirksames Werkzeug um die Verbreitung von Malware, Ransomware und Kryptoviren zu verhindern – im Idealfall ohne dass dabei die Produktivität der Mitarbeiter, die diese Endgeräte nutzen, beeinträchtigt wird.

SCHWACHSTELLE PASSWORT

Die Vielzahl an Produkten und Services, die mittlerweile online zur Verfügung stehen - und durch die Digitalisierung werden es jeden Tag mehr – bringt nicht nur eine steigende Zahl an Zugängen mit sich, sondern auch eine wahre Flut von Passwörtern, die der Sicherung ebendieser Access Points dienen. Das Gefahrenbewusstsein hinsichtlich dieser speziellen Schwachstelle hält mit dieser Entwicklung nicht immer Schritt: In vielen Unternehmen halten sich bis heute schriftliche Notizen oder Excel-Tabellen mit Passwörtern. Viel problematischer sind jedoch meist die Passwörter selbst, die oftmals viel zu einfach sind, obendrein gleich für mehrere Zugänge verwendet werden und selten bis nie geändert werden.

Cybersecurity meets Zeitgeist

Die Cyberkriminellen freut es. Immer mehr Hacker versuchen Zugangsdaten zu stehlen und diese auf digitalen Marktplätzen zu verkaufen. Nicht selten kommt es vor, dass Webseiten gehackt und dadurch ganze Archive mit tausenden Zugangsdaten erbeutet werden - Kombinationen aus Benutzernamen, E-Mail-Adresse und Passwort. Im schlimmsten Fall haben Hacker, falls dasselbe Kennwort tatsächlich mehrmals genutzt worden ist, auch Zugang auf die E-Mail-Adressen und können damit auf Konten, Programme, Tools und Services zugreifen.

Der durchschnittliche Internetnutzer verfügt heute über rund 200 digitale Konten mit zugehörigen Passwörtern. Tendenz steigend. Der Passwortschutz-Anbieter Dashlane macht sich regelmäßig einen Spaß daraus, die unglaublichsten Passwort-Fails aus dem wahren Leben zu veröffentlichen.

So schoss beispielsweise der Hersteller einer beliebten Nuss-Nougat-Creme im Jahr 2018 den Vogel ab, als er auf Twitter seinen Followern allen Ernstes empfahl, „Nutella" als Passwort zu verwenden. Dieser mehr als zweifelhafte Einfall entsprang dem Wunsch des Unternehmens, möglichst öffentlichkeitswirksam den Welt-Passwort-Tag im Mai feiern.

Es handelt sich also durchaus nicht immer um Böswilligkeit, wenn Mitarbeiter Cyberkriminellen durch ihre pure Nachlässigkeit oder Ungeschicklichkeit über ihr Passwort oder ihr Endgerät Tür und Tor zum Unternehmensnetzwerk öffnen.

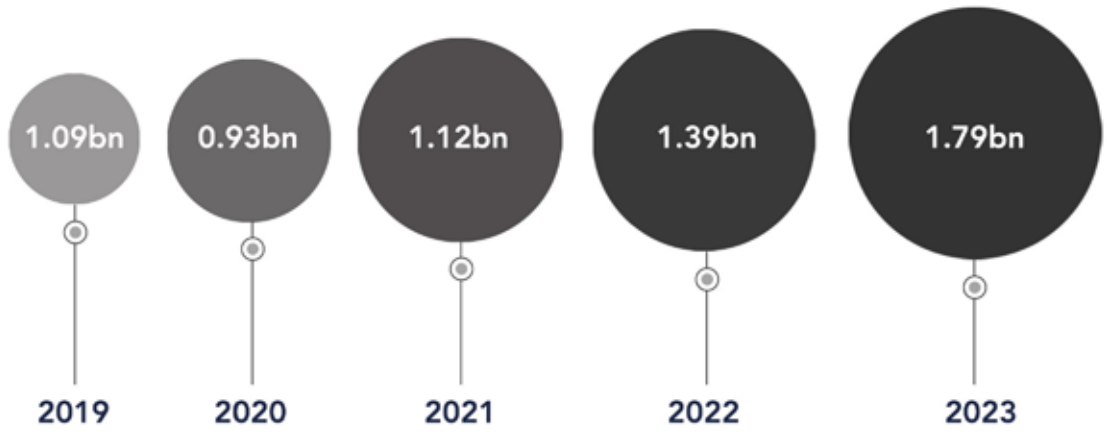
LÖSUNGSANSÄTZE

Für Unternehmen bedeutet dies, dass sie sich immer komplexeren Bedrohungsszenarien gegenübersehen, von denen nichtmal ansatzweise alle in diesem Whitepaper ausführlich vorgestellt wurden. Und täglich werden es mehr. Die wachsende Zahl der sprichwörtlichen offenen Scheunentore wird inzwischen durchaus als Gefahrenquelle wahrgenommen und Maßnahmen zur Sicherung wandern auf der Prioritätenliste immer weiter nach oben.

Das spiegelt sich eindrucksvoll in einer Marktprognose des Security-Analysten KuppingerCole wider, der nicht zuletzt aufgrund der COVID-19 Pandemie enorme Wachstumsraten speziell im Bereich des Access Management vorhersagt:

MARKET SIZE 2019 - 2023

Expected market size in 2019 to 2023, taking a severe market impact of COVID-19 for 2020 into account. CAGR of 13.0% affected by COVID-19 impact in 2020.



Quelle: KuppingerCole Analysist

Dabei stellt das Management privilegierter Zugänge eine Untergruppe des Access Managements dar. Dieses besondere Augenmerk ist nötig, da es sich bei privilegierten Konten in der Regel um eine Art Administrator- oder Superuser-Zugriff handelt, mit dem ein Benutzer überall und jederzeit die vollständige Kontrolle über kritische IT-Systeme und Anwendungen erlangt.

Privileged Account Management (PAM) umfasst eine Reihe von Richtlinien, Prozessen und Tools für den Schutz, die Verwaltung und die Überwachung ebendieser privilegierten Zugriffe, der Benutzer und Anmeldedaten.

Mithilfe von PAM-Lösungen lassen sich diese privilegierten Zugriffe schützen, verwalten und überwachen. Dabei spielt es keine Rolle, ob die privilegierten Accounts – gemeint sind sowohl die von menschlichen als auch von maschinellen Benutzern – sich auf Endpunkten, in Anwendungen oder in der Cloud befinden.

KEY CAPABILITIES - THE FOUR MOST RELEVANT CAPABILITIES OF PAM

01 **Shared Account Password Management**
Managing passwords for shared accounts in a vault, providing secure login to sessions and privileged Single-Sign-On.

02 **Session Management**
Managing, monitoring, and recording of privileged sessions including key management.

03 **Elevated Privilege Management**
Controlling and restricting privileges on target systems in administrative sessions.

04 **Privileged User Behavior Analytics**
Analyzing the behavior of privileged users and identification of anomalies with alerting and interception.

Quelle: KuppingerCole Analysist

PAM-Lösungen ermöglichen es also im Idealfall, alle privilegierten Nutzer in verschiedenen Systemen ohne großen Aufwand zu verwalten. Dazu sollte eine ausgereifte PAM-Anwendung über die folgenden Features verfügen:

- Zugriffe für bestimmte Nutzer auf ausgewählte Systeme limitieren
- Zugang zeitlich auf bestimmte Bereiche gewähren und wieder entziehen
- Überflüssige Passwortverwaltung und Kennworteingaben vermeiden
- Zentrale Verwaltung von Zugriffsrechten über heterogene Netzwerke gewährleisten
- Präzise Audit-Trails für jede Aktion eines privilegierten Nutzers erstellen

Privileged Access Management Suiten gibt es natürlich in verschiedenen Varianten, sollten sich aber immer aus folgenden Bestandteilen zusammensetzen:

- Access Manager – Ein solches Modul reguliert den Zugriff von privilegierten Accounts. An diesem zentralen Punkt werden Richtlinien für das Priviliged Access Management definiert und durchgesetzt. Die Nutzer fragen hier Zugriffsrechte an und der Access Manager erkennt, welche Systeme für einen Nutzer freigegeben sind. Ein spezieller Super Administrator für den Access Manager kann Accounts hinzufügen und löschen oder bestehende Nutzer verwalten. Dadurch wird beispielsweise die Gefahr durch unerlaubte Zugriffe von ehemaligen Mitarbeitern eliminiert. (Eine Bedrohung, die viel größer und realer ist, als viele IT-Manager zugeben wollen.)

- Password Vault – Die Passwörter zu kritischen Systemen müssen geschützt werden, auch vor den Nutzern mit erhöhter Sicherheitsfreigabe. Dadurch können Passwörter nicht ohne Absprache geändert oder überschrieben werden. Die Zugangsdaten sind in einem sicheren Tresor und der Zugang wird erst freigeschaltet, nachdem ein Nutzer diesen beim Access Manager angefragt hat.

- Session Manager – Access Control ist wichtig, aber nicht ausreichend. Der Session Manager bietet die Möglichkeit, die Aktionen eines Anwenders zu verwalten und zu analysieren.

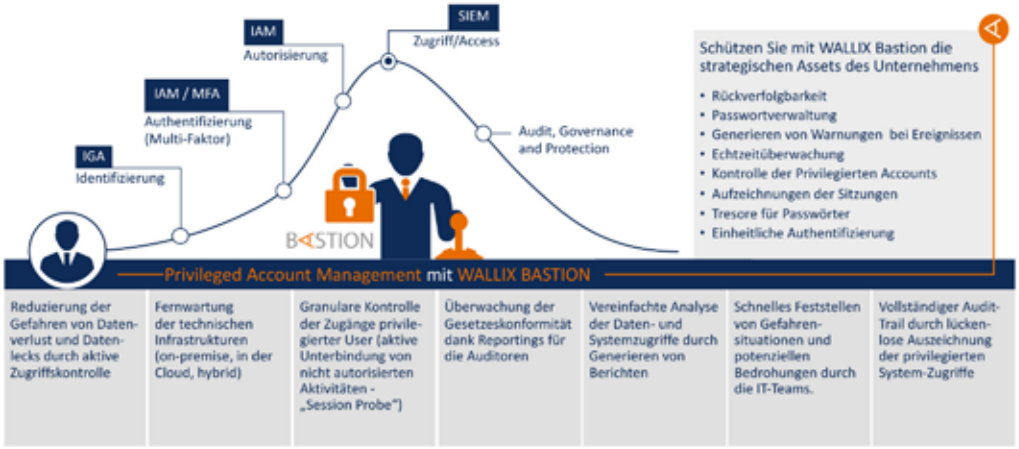
- Endpoint Protection – Endpoints sind Einfallstore für Schadsoftware wie Ransomware, Würmer, Trojaner, Viren oder Spyware und müssen vor der Ausführung und Ausbreitung dieser Malware geschützt werden. Dies erfolgt in zwei Schritten: Zum einen über das „Zero-Trust"-Modell, mit dem sichergestellt wird, dass jeder Benutzer, jede Anwendung und jeder Prozess ausschließlich mit den geringst-notwendigen Berechtigungen auf die Informationen und Ressourcen zugreifen dürfen, die für den jeweiligen Zweck erforderlich sind. Zum anderen mittels der Härtung des Endpoints, um unbekannte oder nicht-autorisierte Prozesse zu blockieren oder aber mit einem Regelwerk zu versehen.

- Identity as a Service (IdaaS) – Sichere Identifizierung des Benutzers ist der höchste Schutz gegen Identitätsdiebstahl. Bereits beim Verbindungsaufbau wird der Benutzer zur Authentifizierung aufgefordert. Die Identität des Benutzers, Ort und Zeitpunkt der Anmeldung sowie die Kritikalität des Zielsystems entscheiden dabei über die Stärke der benötigten Authentifizierung.

Mit Privileged Access Management lassen sich darüber hinaus nicht nur die Konten privilegierter Nutzer verwalten. Vor allem in Kombination mit IdaaS können sämtliche (auch ganz „normale") User sicher angebunden werden. Bei den Zugängen der nicht oder nur in geringem Umfang privilegierten Anwender werden lediglich die Kontrollmaßnahmen reduziert – eine sichere Anbindung ist trotzdem zu jeder Zeit gegeben.

IdM-Lösungen konzentrieren sich auf die grundsätzliche Verwaltung und Beschreibung von Rollenkonzepten, deren Richtlinien und den Benutzern darin. So wird im IdM beispielsweise festgelegt, welche Benutzerprofile nur über PAM Zugang erhalten dürfen.

PAM hingegen konzentriert sich auf den Vorgang des Zugriffs selbst, um diesen gemäß der Security Policies sicher zu gestalten. Man könnte sogar sagen, dass PAM als Polizei oder Wachdienst für IdM fungiert. Bei einem umfassenden Sicherheitskonzept greifen also mehrere Lösungen ineinander: Fernzugriffsschnittstellen in den Firewalls werden wieder vollständig geschlossen. Der Zugriff ist nur noch über einen einzigen Zugang möglich, der engmaschig über PAM und IdaaS überwacht wird.



EUROPÄISCHE HERSTELLER ALS ZUVERLÄSSIGER PARTNER

Nicht erst seitdem der Europäische Gerichtshof (EuGH) im Juli 2020 die Datenschutzvereinbarung "Privacy Shield" gekippt hat, welche die Standards für den Umgang mit europäischen Informationen in den USA festlegt, spielt es für viele Unternehmen mittlerweile eine nicht unerhebliche Rolle, dass die Anbieter von Lösungen zum Schutz der IT Infrastruktur mit ihren teils hochsensiblen Daten nicht aus den USA kommen. Nicht zuletzt deshalb haben sich auch europäische Anbieter wie beispielsweise WALLIX einen festen Platz im Markt erobert. Das Unternehmen weiß um den Wert von Vertrauen. Nicht zuletzt aus diesem Grund unterstützt WALLIX die Europäische Organisation für Computer- und Netzsicherheit (European Cyber Security Organization, ECSO) aktiv. Dabei handelt es sich sozusagen um das privatwirtschaftliche Gegenstück zur Europäischen Kommission für die Umsetzung der vertraglichen öffentlich-privaten Partnerschaft (contractual Public-Private Partnership, cPPP) im Bereich Cybersicherheit.

Cybersecurity meets Zeitgeist

WALLIX trägt insbesondere zur Entwicklung harmonisierter europäischer Kriterien bei, um eine verbesserte Vertrauenszertifizierung für Cybersicherheitslösungen zu erreichen, um so den Kunden die Auswahl von Lösungen zu erleichtern und klar zu zeigen, dass diese Lösungen frei von den berühmt-berüchtigten „Backdoors" sind.

WALLIX bietet Softwarelösungen für Cybersicherheit an und ist Spezialist für die Verwaltung privilegierter Konten. Die Produkte und Lösungen von WALLIX unterstützen die Anwender beim Schutz ihrer kritischen IT-Ressourcen. Zu diesen Produkten gehören unter anderem WALLIX BASTION, eine Privileged Account Management Suite mit Zugriffssicherheit, Kennwortverwaltung, die nach dem Prinzip der geringstmöglichen Rechte funktioniert.

Mit WALLIX BestSafe lassen sich Applikations- und Benutzerprivilegien auf Endpoints managen und so die Verbreitung von Malware, Ransomware und Kryptoviren verhindern, ohne dass dabei die Produktivität der Mitarbeiter beeinträchtigt wird. WALLIX Trustelem schließlich bietet volle Transparenz über die Identität der Nutzer und schützt so die IT-Systeme im Unternehmen wirksam vor Identitätsdiebstahl mit allen seinen unerfreulichen Folgen.

WALLIX PEDM (Privileged Elevation Delegation Management) schließlich stellt sicher, dass privilegierte Berechtigungen nur für die richtigen Konten und zur richtigen Zeit wirken – auch hier ohne negative Effekte auf die Produktivität – und schützt so insbesondere kritische Systeme.

Ein Portfolio wie das von WALLIX macht deutlich, worauf es bei modernen IT Security-Lösungen im Grunde ankommt: Es geht darum, die Komplexität der IT Security Infrastruktur auf ein absolut notwendiges Level zu reduzieren und die volle Kontrolle über sämtliche Access Points zur IT Infrastruktur zu erlangen.

WIRTSCHAFTLICHE BETRACHTUNG

Das ist auch dringend nötig: Nachlässigkeiten beim Thema Zugangskontrolle können enorme wirtschaftliche Auswirkungen haben. Die Schadensvolumina durch Cyberattacken sind immens, man denke nur an Sabotage, Datendiebstahl, Patentrechtsverletzungen oder Spionage.

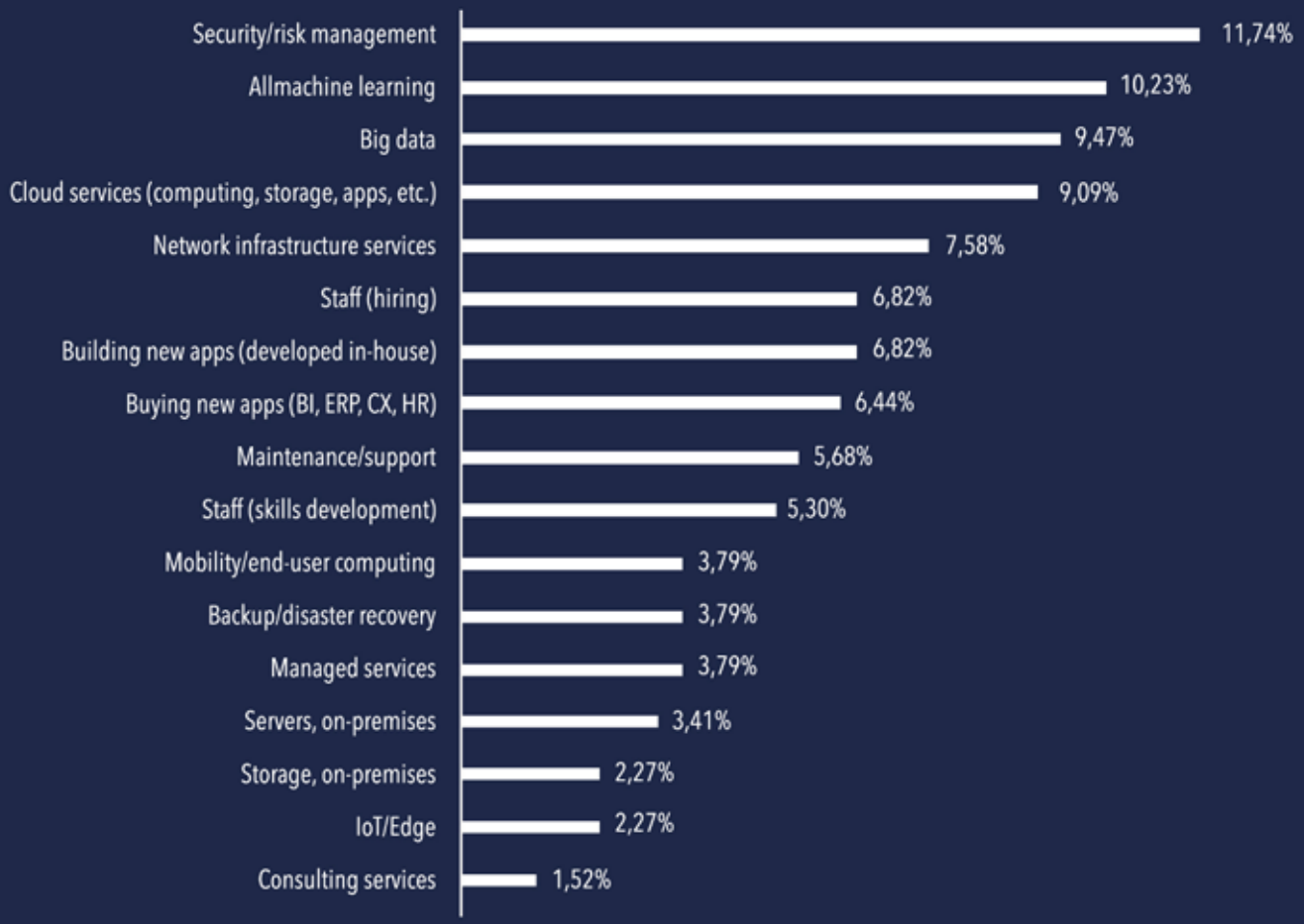
Bitkom beziffert den Gesamtschaden für Deutschland durch Cyberattacken im Jahr 2018 auf über 43 Milliarden Euro. Dazu kommen noch Imageschäden und Vertrauensverluste – die sich eigentlich gar nicht beziffern lassen. Weltweit betrachtet belaufen sich die jährlichen Kosten erfolgreicher Cyber-Angriffe auf eine Summe, die schätzungsweise zwischen 400 Milliarden und 2,2 Billionen US-Dollar liegt, was in etwa dem Bruttoinlandsprodukt von Österreich entspricht.

Es steht zu erwarten, dass sowohl die schiere Anzahl als auch das Ausmaß von Cyberattacken eher noch weiter zunehmen werden.

Informationssicherheitsrisiken sind also Geschäftsrisiken. Das bedeutet aber auch, dass die Verantwortung für diese Risiken nicht allein bei der IT-Abteilung oder dem CIO liegt, sondern mindestens so sehr bei der Geschäftsführung. Und die Dynamik ist enorm: Die Methoden von Cyberattacken ändern sich ständig, das Risiko und die Folgekosten unzureichender Sicherheitsmaßnahmen steigen. Die Vorhersage der nächsten Cyberattacke ist so schwierig wie die des nächsten Erdbebens.

Allerdings ist es nicht zuletzt genau diese Ungewissheit und das mit dem Ernstfall einhergehende Schadensvolumen, das die Unternehmen mehr und mehr zum Umdenken veranlasst. Eine Übersicht der im Jahr 2020 geplanten Investitionen macht überdeutlich, dass in den Unternehmen inzwischen ein Bewusstsein für die Risiken in diesem Bereich vorhanden ist und welchen Stellenwert das Thema Cyber-Security inzwischen hat:

Geplante Investitionen in 2020



Quelle: Flexera 2020 State of Tech Spend Report

Besonders Gewicht erhalten diese Zahlen, wenn man sich vor Augen führt, dass sich die Wirtschaft bedingt durch COVID-19 weltweit mit einer Rezession konfrontiert sieht. Abgesehen davon liegt es angesichts der wirtschaftlichen Schwankungen, die es auch in normalen Zeiten gibt und die keine Organisation beeinflussen kann, gewissermaßen schon in der DNA jedes erfolgreichen Unternehmens, stets mit Bedacht zu investieren.

Tatsächlich rechnet die OECD (Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung) mit einem Einbruch der Weltwirtschaft von bis zu 7,6 Prozent. Corona, so steht es vielerorts zu lesen, löst die schlimmste Rezession seit 100 Jahren aus. Diese durchaus düsteren Prognosen werden dazu führen, dass die Controller in den Unternehmen mit einer deutlich spitzeren Feder rechnen als bisher und mit hoher Wahrscheinlichkeit auch die Ausgaben für die IT-Sicherheit auf ihre Streichliste setzen.

Es steht zu erwarten, dass das Thema Total Cost of Ownership ganz massiv in den Vordergrund rücken wird. Angesichts der hochvolatilen Bedrohungslage, die durch die von den gesellschaftlichen Veränderungen getriebenen Entwicklungen eher immer noch komplexer und unübersichtlicher wird, sind Ansätze gefragt, mit denen sich die Kosten für die Security-Strategie minimieren oder doch immerhin auf dem gleichen Niveau bei gesteigerter Effektivität halten lassen.

Ein solcher, sehr wirkungsvoller Ansatz besteht in der Verringerung der Komplexität der IT-Security-Architektur. Es gilt, die Notwendigkeit bestimmter Applikationen, die dahinter stehenden Personal- und Zeitaufwände (beispielsweise für Auditverfahren oder die Einhaltung von Compliance-Anforderungen wie den Anhang A ISO 27001 oder die DSGVO) und Support-Kosten auf den Prüfstand zu stellen und nach alternativen Lösungen zu suchen.

Ein guter Ansatzpunkt ist die Implementierung einer PAM-Lösung. Sie sollte die höchste Priorität nach Basis-Sicherheitsprogrammen wie der Aktualisierung von Firewalls und Antivirus-Lösungen erhalten. Oder anders ausgedrückt: Die Troika aus Zugangsschutz, Perimeter-Sicherheit und Endpoint Security stellt das unabdingbare Minimum dar und bietet gleichzeitig ein Maximum an Sicherheit. Insbesondere das professionelle Management der Zugänge stellt einen wichtigen Schritt in Richtung weniger Komplexität dar, der zudem auch noch ein höheres Maß an Sicherheit und Benutzerfreundlichkeit mit sich bringt.

Dazu gehört, dass sich eine solche PAM-Lösung in jeder vorhandenen Infrastruktur problemlos installieren lässt und ebenso einfach mit anderen Security Lösungen integriert werden kann - als da wären Firewalls, AntiVirus, SIEM, MFA, Vulnerability Management, IAM, etc. Das ist gerade in der aktuellen Situation, wenn beispielsweise von heute auf morgen mehrere hundert oder sogar tausend Mitarbeiter im Homeoffice sitzen, ein nicht zu unterschätzender Vorteil. Sicherheitslücken sollten tunlichst sofort geschlossen werden. Dabei sollte es idealerweise nicht zu Konflikten zwischen Sicherheit und Produktivität kommen. Denn in der Regel bedeutet optimale Produktivität leider auch Reduzierung der Sicherheit und umgekehrt.

In Kombination mit PAM ist es jedoch möglich, die Sicherheitseinstellungen von Basis-Sicherheits-programmen (wie Firewalls) zu maximieren, da sämtliche Zugänge zu geschäftskritischen Ressourcen über PAM-Portale gesteuert werden. Somit entfällt der Konflikt zwischen hoher Perimeter-Sicherheit und den geschäftsrelevanten Zugriffsprozessen.

IT-SECURITY VON HEUTE

CORONA

Digitalisierung auf dem Weg
in unsere DNA

Betreiber / Anwenderverhalten
Auswirkung (z.B. Remote Life)

KRITIS im neuen Licht
Stichwort Systemrelevanz

ÖKONOMIE

Rezession schärft Blick auf TCO,
Konsolidierung

Kosten-Nutzen-Analysen
werden kritisch

Aktives Risikomanagement
als Prävention

REGULARIEN

Compliance Anforderungen

EU vs. den Rest der Welt
Industrie, Staat, nationale und lokale
Anforderungen

KOMPLEXITÄT

Hybrid IT - DevOps

IT to OT and IOT
Mobility
Interoperabilität

DER AUSBLICK

Machen wir uns nichts vor. Die nächste große Revolution ist längst in vollem Gang und hat durch COVID-19 noch einmal deutlich an Fahrt aufgenommen. Der Zeitgeist des „Anything Goes" beschreibt die gesellschaftliche Grundstimmung und umreißt die fundamentalen Veränderungen in der Art wie wir leben und arbeiten. Auch das IoT, das komplett ohne Menschen auskommt, ist auf dem Vormarsch und exponentiell wachsende Datenberge sind die sichtbare Folge der Digitalisierung.

Diese raumgreifende Vernetzung von allem mit allen birgt immer neue Gefahren für Endnutzer und Unternehmen. „Die Revolution frisst ihre Kinder", lautet ein geflügeltes Wort und es besagt, dass etwas, das positiv begonnen hat, in etwas Negatives umschlägt.

Um das zu verhindern und um das nicht enden wollende Hase-und-Igel Spiel, das sich Cyberkriminelle und ihre Opfer liefern, zu gewinnen, müssen die Unternehmen ihre Sicherheitsstrategien auf den Prüfstand stellen, Gewohntes und Eingefahrenes hinterfragen und die Herausforderungen nehmen. Sich dem Zeitgeist stellen, sozusagen.

about WALLIX

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED