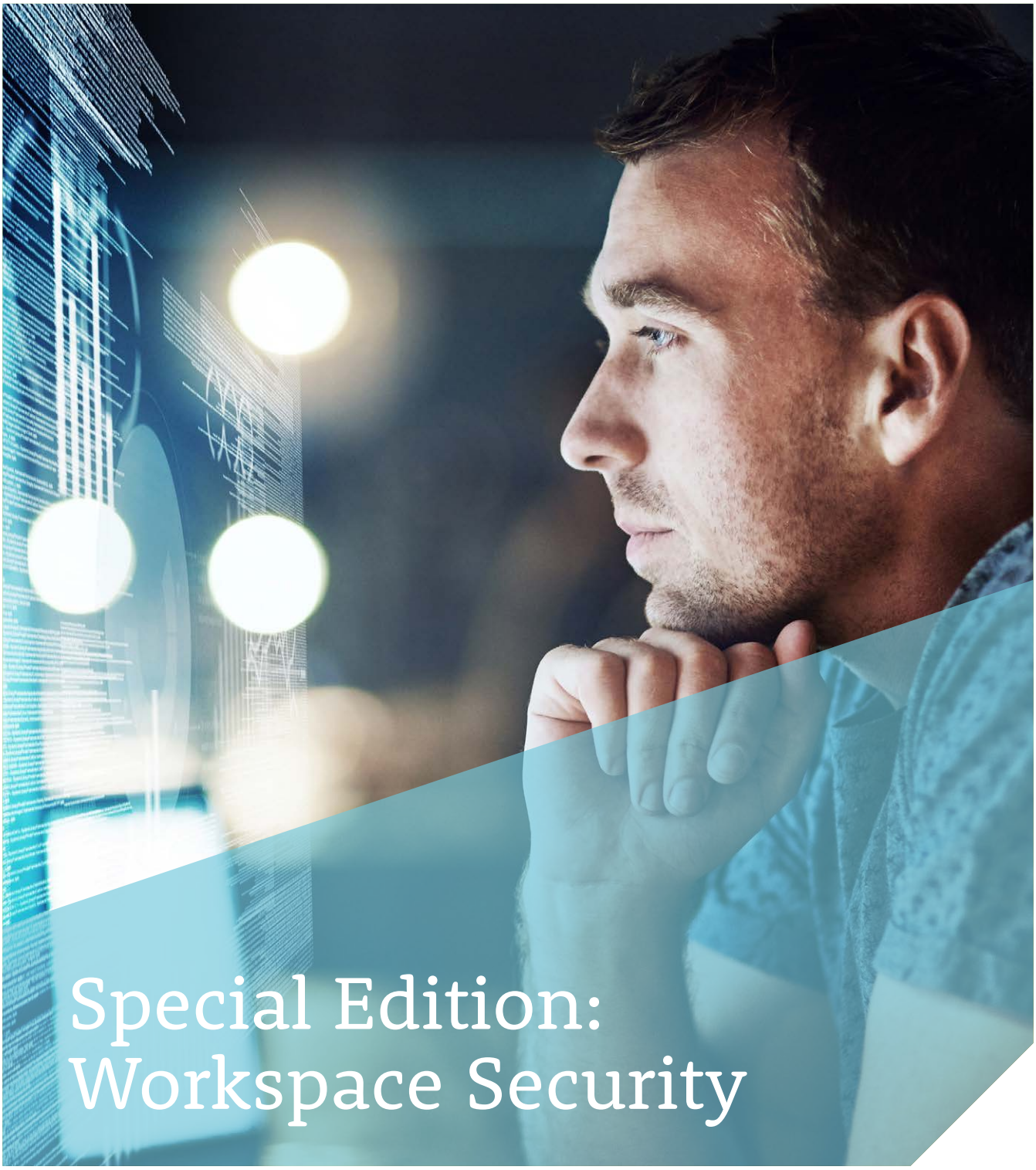
Digital Workspace



Special Edition: Workspace Security

//SVA TechCompass

Management Summary

Hybrid arbeiten – und das mit Begeisterung! Der digitale Arbeitsplatz hat mittlerweile in vielen Unternehmen eine Qualität erreicht, die Mitarbeitenden die gewünschte Flexibilität bietet, um Aufgaben auch außerhalb der Büroräumlichkeiten schnell, effizient und ohne technische Zipperlein zu erledigen. Doch wie bei so vielem steht auch die Entwicklung des Digital Workspace nicht still: Stetig kommen neue Lösungen auf den Markt, die es wert sind, integriert zu werden. Gleichzeitig wandeln sich die unternehmerischen Anforderungen unentwegt, was eine kontinuierliche Anpassung der digitalen Arbeitsplatzumgebung erforderlich macht.

Vor allem das Thema Sicherheit ist angesichts der aktuellen IT-Bedrohungslage immer wieder neu zu bewerten. Denn bei allen Vorteilen schafft der Digital Workspace auch neue, sich stetig verändernde Angriffsvektoren, die nur durch konsequente Digital- und Security-Strategien in Verbindung mit modernen Sicherheitsansätzen geschlossen werden können. Das Management und die IT-Abteilungen sind somit gefordert, zusammenzuarbeiten und sich der Absicherung des Arbeitsplatzes zielgerichtet und mit Weitblick anzunehmen, um nicht nur jetzt, sondern auch in Zukunft von seinen Mehrwerten profitieren zu können.

Dem Sicherheitskonzept Zero Trust kommt hierbei eine besondere Bedeutung zu, denn es ist auf alle Bereiche anwendbar, die im Kontext Workspace Security von Relevanz sind. Ob Mobile Threat Defense, Identitätsmanagement, eine passwortlose Authentifizierung oder eine rollenbasierte Zugriffskontrolle, die den Standort des Nutzers miteinschließt – all diese modernen Ansätze und Lösungen orientieren sich an den Zero-Trust-Leitprinzipien und tragen dazu bei, ein wirksames Schutzschild aufzubauen. Der Clou liegt darin, die für sich passenden Technologien aufzuspüren und so miteinander zu verzahnen, dass eine Architektur entsteht, die jedem noch so starken Erdbeben standhält. Cyberresilienz ist das Gebot der Stunde – und die Uhr tickt.

Inhalt

1/ Worum es geht. Eine kurze Einführung. 5

// Hybrid Work: Vom Trend zum Standard 5

// Workspace Security: Von der Kür zur Pflicht 6

// Inhalt dieser Ausgabe 7

2/ IT-Sicherheit in Unternehmen. Status quo. 8

// Deutschland als Hotspot 9

// Die Organisation als Angriffsziel 11

// Der Mensch als Teilchenbeschleuniger 16

3/ Zero Trust. Vertraue niemandem. 18

4/ Workspace Security. Ansatzpunkte zur Optimierung. 21

// Identity Security 22

// Endpoint Security 26

// Network Security 30

// Application Security 34

// Data Security 37

// Security Awareness 40

// Security Monitoring & Reporting 42

5/ Der Blick in die Zukunft. Spannend und wertvoll. 46

6/ Resümee. Bleiben Sie sicher unterwegs! 49

7/ SVA. Ihr kompetenter Ansprechpartner. 50

1/ Worum es geht.
Eine kurze Einführung.

Wir alle lieben das Gefühl von Sicherheit. Und entsprechend strebt jeder von uns unwillkürlich danach, ein Leben zu führen, das stets frei ist von jeglichen inneren und äußeren Gefahren. Doch so sehr wir uns ein beschütztes Dasein wünschen, so sehr werden wir jeden Tag aufs Neue mit der Realität konfrontiert. Der deutsche Schriftsteller Joachim Ringelnatz hat es bereits vor 100 Jahren auf den Punkt gebracht: „Sicher ist, dass nichts sicher ist." – und diese wahren Worte lassen sich heute nicht nur allgemein auf das Leben, sondern ganz besonders auch auf die IT anwenden.

In seinem Lagebericht von 2023 spricht das Bundesamt für Sicherheit in der Informationstechnik (BSI) von einer angespannten bis kritischen IT-Sicherheitslage in Deutschland[1]. Dies liegt vor allem in der zunehmenden Digitalisierung und Vernetzung begründet, die – bei allen Chancen, die sie bietet – leider auch immer wieder neue und größere Angriffsziele schafft. Dabei sind Organisationen besonders hohen Sicherheitsrisiken ausgesetzt, denn notwendige Initiativen wie beispielsweise die Digitalisierung des Arbeitsplatzes, verbunden mit der Möglichkeit eines ortsunabhängigen Arbeitens, verführen Cyberkriminelle regelrecht zu illegalen Machenschaften. Wer da nicht handelt, hat schon verloren.

// Hybrid Work: Vom Trend zum Standard

Kaum etwas hat sich in den vergangenen Jahren so in seinen Grundfesten geändert wie die Art, wie wir heute arbeiten. Die Coronapandemie zwang Unternehmen, in aller Eile digital aufzurüsten und ihren Mitarbeitenden die Arbeit von zuhause zu ermöglichen. Damit brach sie eine Entwicklung los, die sich zwar lange abzeichnete, aber selbst die ambitioniertesten Visionäre in ihrer Wucht überraschte.

Denn was ursprünglich als vorübergehende Präventionsmaßnahme angedacht war, sollte sich als Dauerzustand erweisen. Mit Fortschreiten der Pandemie hat sich das mobile Arbeiten in vielen Organisationen zum Standard entwickelt. Gleichzeitig wurde das Homeoffice zum bevorzugten Ort der Schaffenskraft, auf den Mitarbeitende auch heute nicht mehr verzichten wollen. Der Weg war frei für Hybrid Work – ein Ansatz, der mittlerweile bei der Mehrheit großer und mittlerer deutscher Unternehmen zu einer Selbstverständlichkeit geworden ist[2] und sich zweifelsohne auch bei kleineren Firmen mehr und mehr durchsetzen wird.

[1] *Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2023*

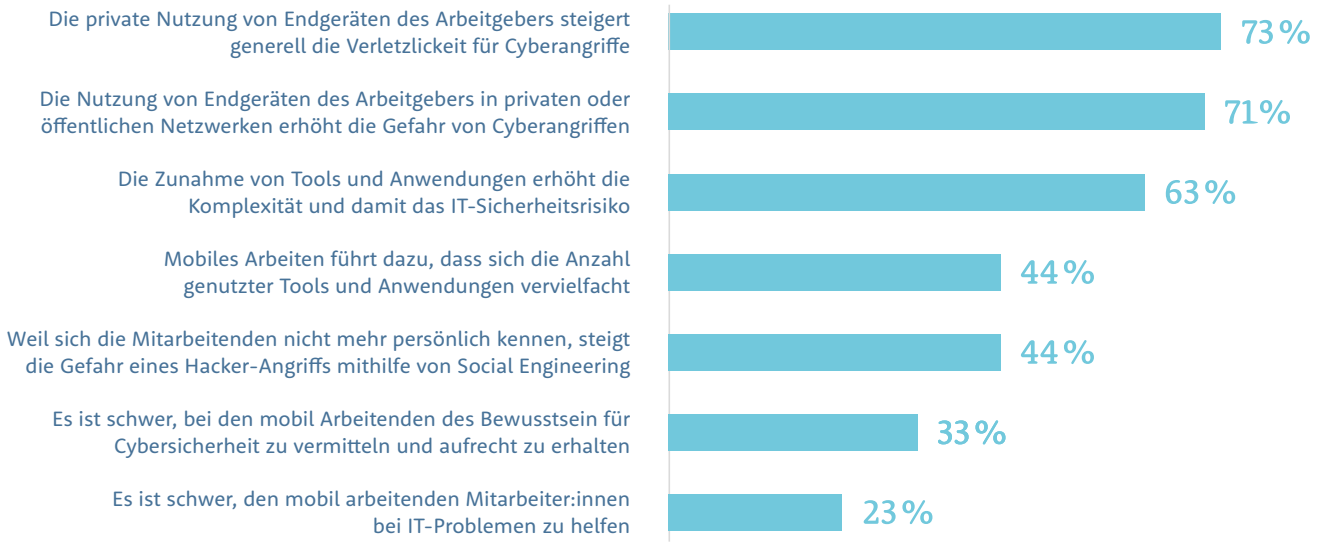
[2] *TÜV, Cybersecurity Studie 2023*

// Workspace Security: Von der Kür zur Pflicht

Mit der Etablierung hybrider Arbeitsweisen steigen unweigerlich die Anforderungen an die Absicherung des digitalen Arbeitsplatzes. Denn mit jedem neuen Endgerät und jeder weiteren Anwendung, die mobiles Arbeiten möglich machen soll, geht automatisch eine gesteigerte Komplexität der Infrastruktur einher, was sie wiederum anfälliger für Cyberangriffe macht.

Entsprechend sind Unternehmen heute mehr denn je gefordert, wirksame Vorkehrungen zu treffen, damit aus keinem noch so kleinen Sicherheitsrisiko ein Sicherheitsfiasko wird. So braucht es zum einen präventive und reaktive Sicherheitsstrategien, die den Digital Workspace in seiner Gesamtheit betrachten und dabei bestenfalls jede Art von möglichen Sicherheitsvorkommnissen berücksichtigen. Zum anderen sind für die strategische Umsetzung aktuelle IT-Security-Technologien notwendig, die in der Lage sind, schnell und wirksam auf Angriffe zu reagieren und sie möglichst schon im Keim zu ersticken. Klar ist: Die Liste an zu treffenden Schutzmaßnahmen ist lang. Klar ist aber auch, dass jede von ihnen dazu beiträgt, ein Stück sicherer unterwegs zu sein.

Welche Risiken für Cybersicherheit birgt aus Ihrer Sicht mobiles Arbeiten?



Basis: n=501
Quelle: TÜV, Cybersecurity Studie 2023

// Inhalt dieser Ausgabe

Dass Workspace Security ganz oben auf die Agenda von IT-Abteilungen gehört, ist kein Geheimnis. Und doch scheuen sich noch immer viele Unternehmen davor, das Thema beherzt anzugehen und weiter zu forcieren. Diese Zurückhaltung ist in aller Regel fehlenden Personalressourcen geschuldet, genauso wie dem Umstand, dass die Möglichkeiten einer Absicherung des digitalen Arbeitsplatzes so enorm vielfältig sind. Folglich weiß man gar nicht, wo man anfangen soll.

Mit dieser Sonderausgabe des SVA TechCompass möchten wir das ändern. Sie soll Ihnen als Leitfaden dienen, der aufzeigt, welche Bereiche von sicherheitsrelevanter Bedeutung sind und mit welchen Schutzmaßnahmen Sie es schaffen, die Cyberresilienz Ihrer digitalen Arbeitsplatzumgebung zu erhöhen. Dazu werfen wir zunächst einen Blick auf die allgemeine IT-Bedrohungslage sowohl in Deutschland als auch speziell in der deutschen Wirtschaft. Im Anschluss wenden wir uns dem Sicherheitskonzept Zero Trust zu und gehen auf seine konkrete Anwendbarkeit im Digital-Workspace-Kontext ein. Hierbei erhalten Sie nicht nur einen Überblick über alle schützenswerten Bereiche, sondern auch hilfreiche Ansatzpunkte zu deren Optimierung.

2/ IT-Sicherheit in Unternehmen.

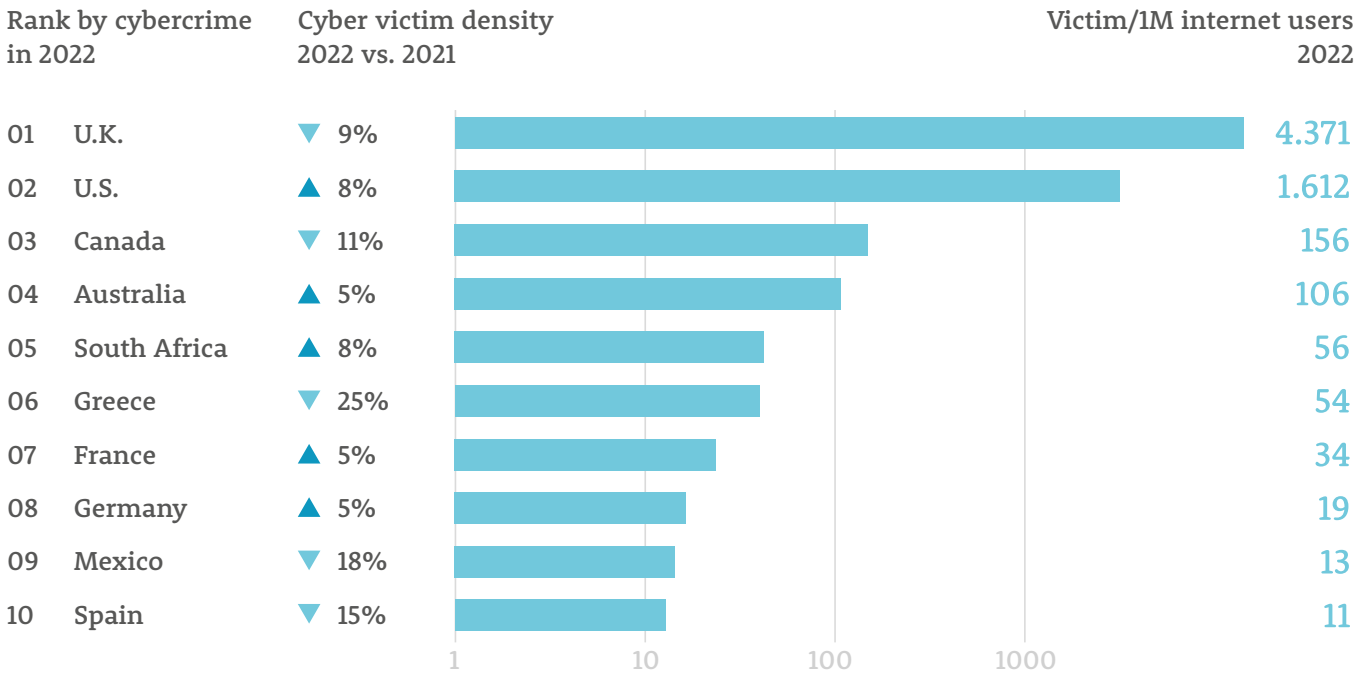
Status quo.

Die Geschichte von ‚David gegen Goliath' ist weltbekannt: Der vermeintlich schwächere Hirte David kämpft gegen den übergroßen Gegner Goliath und schafft, nur mit dem Einsatz seines Verstandes, am Ende das, was vorher unmöglich schien – den Sieg. Diese Botschaft, inspirierend und motivierend zugleich, ist ein schönes Sinnbild dafür, was Unternehmen im Kampf gegen die scheinbar vorherrschende Cyberkriminalität erreichen können. Kennt man den Gegner und weiß ihn einzuschätzen, kennt man die Gefahren und weiß um ihr Ausmaß, so lässt sich mit diesem Wissen die richtige Taktik entwerfen, um fortan für jede Art von Bedrohung gewappnet zu sein. **Werfen wir also einen Blick auf die aktuelle Gefahrenlage.**

// Deutschland als Hotspot

Deutschland zählt – wirtschaftlich gesehen – zu den Big Playern weltweit. Entsprechend dürfte es nicht überraschen, dass unser Land auch bei Cyberkriminellen hoch im Kurs steht. Laut BSI war die Bedrohung im Cyberraum Deutschland noch nie so groß wie heute, die Zahl der Angriffe und die Vielfalt der eingesetzten Methoden noch nie so ausgeprägt wie in der aktuellen Zeit[3]. Zahlreiche Studien, darunter die Analyse des IT-Security-Unternehmens Surfshark, sehen Deutschland sogar unter den Top-10 der Länder, die die höchste Cyberkriminalität aufweisen[4].

Top 10 countries by cybercrime density



[3] *Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2023*

[4] *Surfshark, Cybercrime statistics (https://surfshark.com/research data-breach-impact/statistics)*

Forciert wird die ohnehin schon angespannte IT-Sicherheitslage durch die rasante Weiterentwicklung neuer und angepasster Angriffsmethoden. Hierbei gelten die altbekannten Ransomware-, DDoS- und Phishing-Attacken zwar noch immer als Hauptbedrohung, werden aber zunehmend um neue, vor allem durch KI-optimierte Varianten ergänzt. Einen weiteren Anlass zur Sorge bietet zudem die fortschreitende Professionalisierung der Cyberkriminalität: Cybercrime als Dienstleistung (Cybercrime as a Service, CCaaS) ist auf dem Vormarsch und wird die aktuelle Bedrohungssituation für Deutschland weiter verschärfen.

Dies wäre jedoch alles nicht so schlimm, wenn es da nicht den besorgniserregenden Anstieg im Bereich der Software-Schwachstellen gäbe, die oftmals als erstes Einfallstor zur Kompromittierung von Systemen und Netzwerken dienen. So wurden nach Aussagen des BSI im Berichtszeitraum von Juni 2022 bis Juni 2023 täglich knapp 70 neue Sicherheitslücken in jeglicher Art von Softwareprodukten entdeckt – ein Zuwachs von 24 Prozent im Vergleich zum vorherigen Zeitraum. Diese insgesamt 27.000 neuen Schwachstellen waren zu 15 Prozent kritischer Natur und betrafen sowohl spezialisierte Fachanwendungen als auch komplexe Serverstrukturen und Handy-Apps.

Was lernen wir also daraus? Dass es keinen Grund gibt, sich in Sicherheit zu wiegen? Dass jeder in Deutschland potenziell gefährdet ist, sei es der typische Verbraucher oder ganze Organisationen? Nein, denn diese Erkenntnisse sind nicht neu. Viel wichtiger ist zu verstehen, dass sich die Gefahren dynamisch entfalten, dadurch schwer zu fassen und zu bändigen sind und man somit per se auf alle Eventualitäten vorbereitet sein muss. Im nächsten Abschnitt beleuchten wir, wie Unternehmen mit dieser Situation umgehen.

Cybercrime as a Service (CCaaS)

CCaaS steht für einen Ansatz, der es einem Angreifer erlaubt, nahezu jeden Schritt eines Angriffs als Dienstleistung von anderen Cyberkriminellen zu beziehen. Auf diese Weise können sich Angreifer auf bestimmte Dienstleistungen spezialisieren, diese gezielt entwickeln und ihre Effizienz steigern. Weiterhin stehen die Dienstleistungen vielen weiteren Angreifern gleichzeitig zur Verfügung, wodurch sich der Zeitraum zwischen der Entwicklung einer neuen Methode und deren Einsatz stark verkürzt bzw. ganz wegfällt.

// Die Organisation als Angriffsziel

Innovationskraft, Stabilität, globale Vernetzung – deutsche Unternehmen gelten als leistungsstark, was sie zu einem attraktiven Angriffsziel für Hacker aus aller Welt macht. Deutschlands Wirtschaft steht buchstäblich unter Beschuss. Und hiervon betroffen sind nicht ausschließlich internationale Großkonzerne, sondern Institutionen jeder Art und Größe.

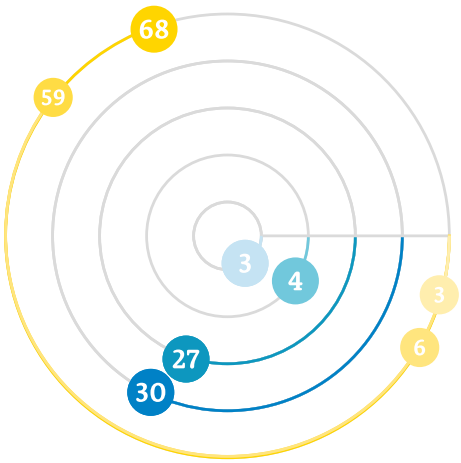
In seinem Lagebericht von 2023 spricht das BSI von einem Trend, wonach sich cyberkriminelle Angreifer verstärkt auf solche Opfer konzentrieren, die ihnen leicht angreifbar erscheinen.[5] Ins Visier geraten nun vermehrt kleine und mittlere Unternehmen (KMU), Behörden der Landes- und Kommunalverwaltungen, wissenschaftliche Einrichtungen und KRITIS-Unternehmen wie Krankenhäuer, die eine ideale Fläche bieten, um Angriffe mit wenig Aufwand, dafür aber mit großem Nutzen zu platzieren.

Befragt man Organisationen zur eigenen Sicherheitslage, so wird schnell deutlich, dass nahezu jede von ihnen schon einmal von einem Angriff betroffen war. Gut jedes zehnte Unternehmen (11 %) hatte in den letzten zwölf Monaten mit einem, jedes zwanzigste Unternehmen (5 %) sogar mit mehr als einem IT-Sicherheitsvorfall zu kämpfen.[6] Hierbei hatten es Angreifer überproportional häufig auf große Organisationen mit mehr als 250 Mitarbeitenden abgesehen (19 %).

Auch hinsichtlich der Angriffsmethoden gibt es offensichtlich Präferenzen seitens der Angreifer – von Malware bis hin zur persönlichen Manipulation. So wurde der Großteil der betroffenen Unternehmen in der Vergangenheit Opfer von Phishing- oder Spear-Phishing-Angriffen, die darauf abzielen, mittels entwendeter Zugangsdaten Zugriff auf relevante Systeme zu erlangen. Weiterhin sind Ransomware-Attacken in Verbindung mit Lösegeldforderungen noch immer bei Cyberkriminellen beliebt, dicht gefolgt vom Social Engineering, bei dem Beschäftigte manipuliert werden, um sich Zugang zur Unternehmens-IT zu verschaffen.

Bekannt gewordene Ransomware-Opfer in Deutschland im Berichtszeitraum

nach Art des Opfers (Anzahl)



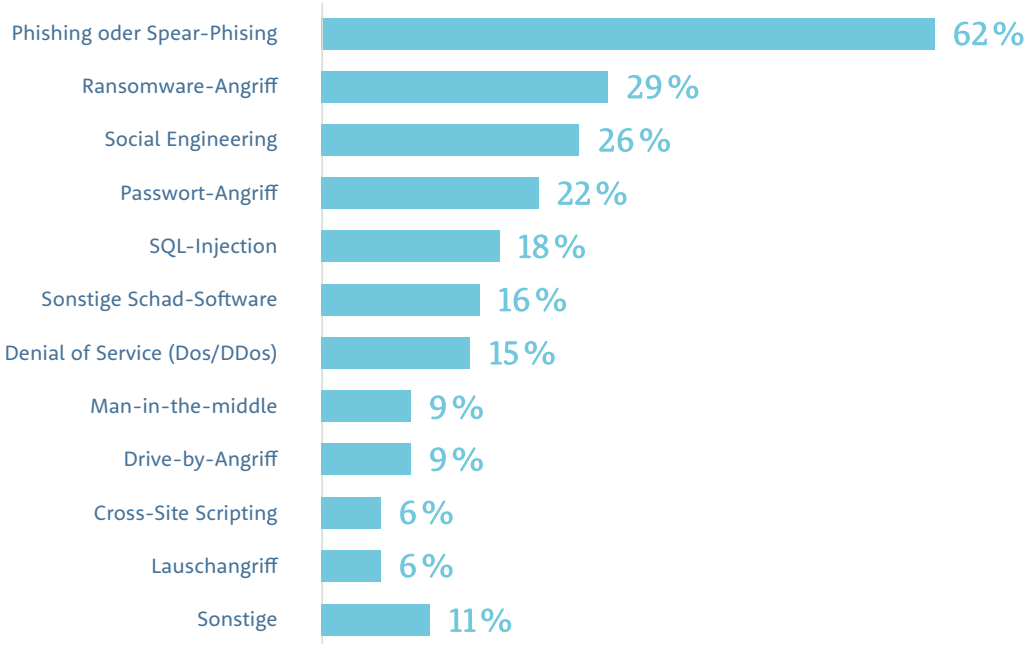
- Sonstige
- Krankenhäuser
- Kommunen, kommunale Betriebe
- Forschungs-und Bildungseinrichtungen
- Andere
  - Mittlere Unternehmen
  - Große Unternehmen
  - Kleine, Kleinstunternehmen

Quelle: Ransomware-Opfer-Statistik des BSI

[5] *Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2023*

[6] *TÜV, Cybersecurity Studie 2023*

Art der IT-Sicherheitsvorfälle bei betroffenen Unternehmen



Quelle: TÜV, Cybersecurity Studie 2023

Die finanziellen Schäden, die Cyberattacken in der deutschen Wirtschaft anrichten, sind hierbei beträchtlich. Nach Schätzungen des Digitalverbandes Bitkom haben Unternehmen im Jahr 2022 einen Gesamtschaden von rund 206 Milliarden Euro durch Angriffe erlitten – Tendenz steigend.[7]

Die gute Nachricht ist: Die Mehrheit der deutschen Organisationen hat die Bedeutung von Cybersecurity erkannt und in entsprechende Schutzmaßnahmen investiert. Seit 2020 sind die Ausgaben für das IT-Sicherheitsbudget in Unternehmen kontinuierlich gestiegen; 2022 wurde mit rund 7,8 Milliarden Euro so viel wie noch nie für Cybersicherheit ausgegeben.[8] Zudem ist zu erwarten, dass die Investitionsbereitschaft weiterhin steigt, was angesichts der jährlichen Schadenssumme mehr als notwendig ist, um die eigene Existenz nicht zu gefährden.

[7] *Bitkom, Studie Wirtschaftsschutz 2023*
[8] *Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2023*

Schaden durch ...	Schadenssumme in Mrd. Euro (2023)	Schadenssumme in Mrd. Euro (2022)
Imageschaden bei Kunden oder Lieferanten, negative Medienberichterstattung	35,3	23,6
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	35,0	41,5
Kosten für Rechtsstreitigkeiten	29,8	16,2
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	25,2	10,1
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	21,5	41,5
Kosten für Ermittlungen und Ersatzmaßnahmen	16,1	10,7
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	15,3	21,1
Datenschutzrechtliche Maßnahmen (z. B. Informationen von Kunden)	12,4	18,3
Patentrechtsverletzungen (auch schon vor der Anmeldung)	10,4	18,3
Geldabfluss durch Betrugsversuche	3,9	–
Sonstige Schäden	1,1	0,9
Gesamtschaden pro Jahr	205,9	202,7

Quelle: Bitkom

Brennpunkt: Workspace Security

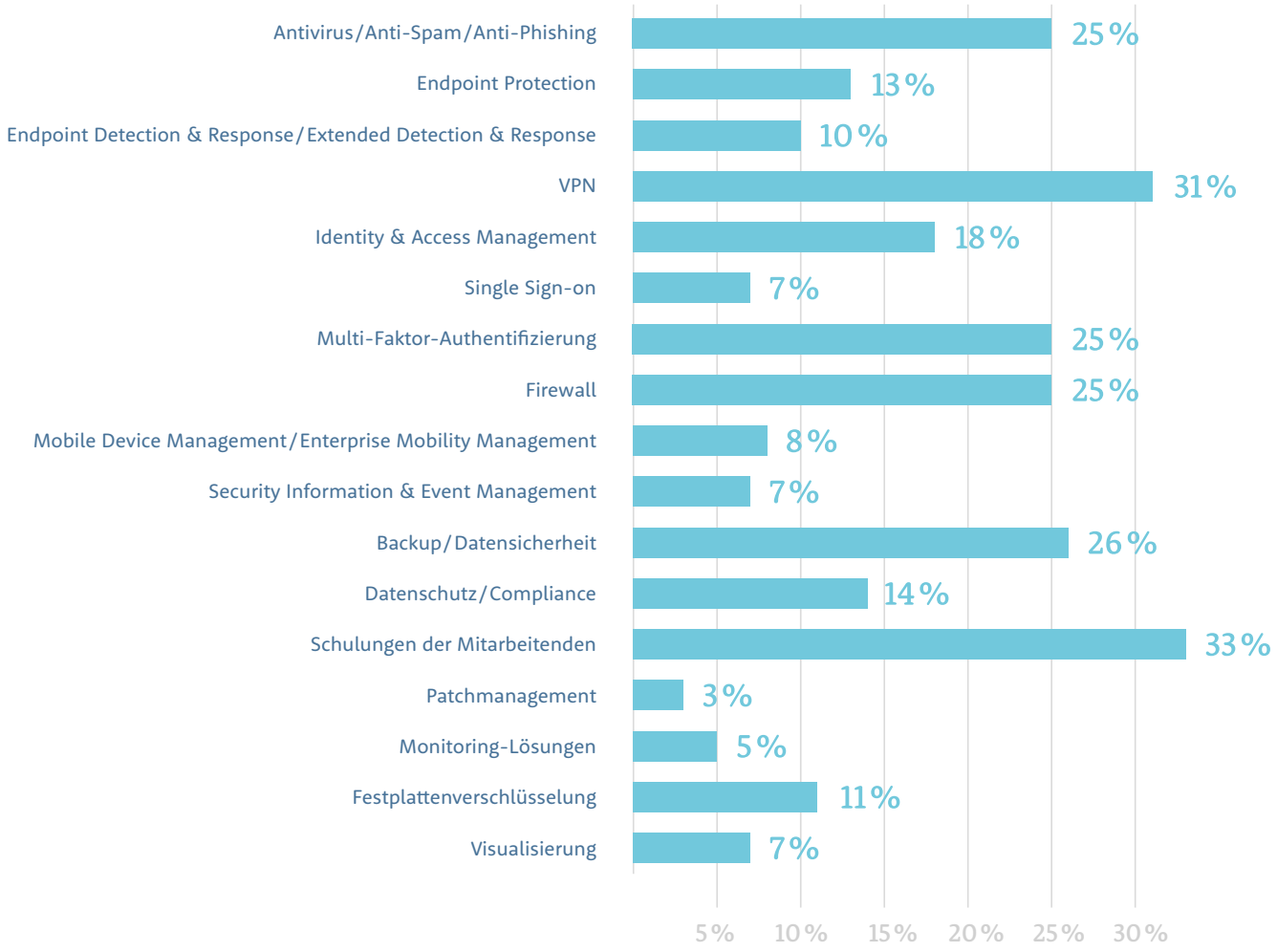
IT-Sicherheit steht bei vielen Unternehmen mittlerweile ganz oben auf der Agenda. Doch inwieweit werden dabei auch flexible Arbeitskonzepte berücksichtigt? Und auf welche Technologien und Maßnahmen wird bevorzugt zurückgegriffen, um den digitalen Arbeitsplatz ausreichend abzusichern? Um diese Fragen zu klären, hilft ein Blick in aktuelle Statistiken.

Generell stehen die Zeichen auf positiv: Laut einer Studie der WEKA Fachmedien sehen sich knapp ein Fünftel der befragten Unternehmen im Hinblick auf hybride Arbeitskonzepte bei der IT-Sicherheit als optimal, mehr als die Hälfte immerhin als sehr gut aufgestellt – jedoch mit Entwicklungsbedarf. Dies ist auch nicht verwunderlich, da die Zahl der Angriffe vor allem auf Heimarbeitsplätze gestiegen ist und Unternehmen somit nicht umhin kommen, ihre IT-Sicherheitsstrategie fortlaufend weiterzuentwickeln und Lösungen zu modernisieren.

Interessant ist in diesem Zusammenhang, auf welche Bereiche und Technologien IT-Abteilungen aktuell setzen, um ihre Infrastruktur zu schützen: Noch immer werden VPN- und die grundlegenden IT-Sicherheitslösungen Antivirus, Firewall und Backup präferiert, obwohl insbesondere für VPN schon deutlich wirksamere Alternativen existieren (siehe ‚ZTNA schlägt VPN', Seite 33) Gleichzeitig scheinen Unternehmen die Dringlichkeit erkannt zu haben, ihre digitalen Identitäten ganzheitlich abzusichern, denn sowohl Identity & Access Management als auch Multi-Faktor-Authentifizierung sind klar auf dem Vormarsch. Weniger beliebt sind hingegen der Schutz der Endgeräte, Patchmanagement und Security-Monitoring – ein Umstand, der aufhorchen lässt und in Anbetracht der hohen Sicherheitsrelevanz aller drei Maßnahmen unbedingt geändert werden sollte.

Aus Unternehmenssicht relevante IT-Security-Technologien/ -Bereiche zum Schutz von Digital-Workspace-Strukturen

inkl. mobiler Arbeitsplätze



Basis: n=242
Quelle: WEKA Fachmedien, Studie Digital Workplace 2021/2022

[9] *Heise Online, Artikel „Continental: IT-Einbruch erfolgte über heruntergeladenen Browser von Mitarbeiter“*
[10] *Bayerischer Rundfunk, Mitteilung „Phishing-Vorfall beim BR“*
[11] *HHU Düsseldorf, Mitteilung „Daten aus E-Mails der HHU entwendet“*

Es kann jeden treffen – Drei prominente Opfer

Continental
Im Juli 2022 wurde Continental zum Ziel von Cyberkriminellen. Hierbei ist es einer Hackergruppe trotz umfassender Sicherheitsvorkehrungen seitens des Automobilzulieferers gelungen, Ransomware in Form eines nicht autorisierten Browsers einzuschleusen, der durch einen Beschäftigten unbeabsichtigt ausgeführt wurde. Auf diese Weise gelangten die Kriminellen an den Benutzeraccount und das Passwort des Mitarbeiters, womit sie sich Zugang zu wichtigen Continental-Systemen verschafften. Sie hielten sich etwa einen Monat lang unentdeckt im Conti-Netz auf und erbeuteten 40 TB Daten – darunter Daten von Continental selbst als auch personenbezogene Daten aktiver und ehemaliger Mitarbeitender. Auf das geforderte Lösegeld ging der Konzern nicht ein.[9]

Bayerischer Rundfunk (BR)
Der Bayerische Rundfunk wurde im Februar 2023 von einem Phishing-Angriff getroffen. Laut Angaben des Medienhauses wurden einzelne Mitarbeitende durch plausibel gestaltete E-Mails getäuscht und dann auf eine echt aussehende Eingabemaske mit BR-Logo weitergeleitet. Durch die eingegebenen Login-Daten erhielten die Betrüger zwischenzeitlich Zugriff auf interne und externe Adressbuch-Kontakte, den E-Mail-Verkehr und weitere Speicherorte. Die Sicherheitslücke wurde unverzüglich nach dem Vorfall geschlossen. Ein Abfluss von Daten konnte nicht ausgeschlossen werden.[10]

HHU Düsseldorf
An der Heinrich-Heine-Universität Düsseldorf wurde im Mai 2023 ein einzelnes IT-Arbeitsplatzsystem durch einen Angriff mit einer Schadsoftware kompromittiert. Als Folge erhielten die Angreifer zunächst unbemerkt Zugriff auf die E-Mail-Postfächer, die im entsprechenden System eingebunden waren. Im weiteren Verlauf wurden die Inhalte der entwendeten Mails für Phishing-Angriffe auf Kontakte der Postfächer innerhalb und außerhalb der HHU genutzt. Die Schließung der Sicherheitslücke erfolgte unmittelbar nach ihrem Bekanntwerden.[11]

// Der Mensch als Teilchenbeschleuniger

Wir Menschen machen Fehler. Ob bewusst oder unbewusst. Und Angreifer machen sich diese Schwäche immer mehr zunutze. In der Tat gilt der Mensch heute als mitunter größtes IT-Sicherheitsrisiko, denn je digitaler er unterwegs ist und je mehr Endgeräte er dafür nutzt, desto mehr potenzielle Angriffsfläche stellt er Kriminellen zur Verfügung.

Entsprechend sind Social-Engineering-Angriffe schwer im Kommen, die bewusst auf die Manipulation von uns Menschen abzielen, um sich unerlaubten Zugang zu Systemen zu verschaffen. Phishing-Mails, also E-Mails mit betrügerischen Absichten, gelten laut BSI neben Ransomware mittlerweile als Hauptbedrohung; der TÜV-Verband stuft sie sogar anhand einer Unternehmensumfrage als die Methode ein, von der Organisationen mit Abstand am häufigsten betroffen sind.[12] Hinzu kommen Angriffsvariationen wie Smishing (Phishing per SMS) und Vishing (Voice Phishing), die zwar andere Kanäle nutzen, aber auf dasselbe Ziel einzahlen: den Empfänger mittels Kurz- oder Sprachnachricht dazu zu verleiten, einen Link zu klicken, hinter dem sich schädliche Apps oder maliziöse Webseiten befinden.

Der Umgang mit Phishing ist für Unternehmen nicht grundsätzlich neu. Schaut man jedoch auf die technologischen Entwicklungen der letzten Monate und das insbesondere im Bereich der Künstlichen Intelligenz (KI), so braucht es keine Glaskugel, um vorhersagen zu können, dass die Qualität der Phishing-Attacken eine neue Dimension erreichen wird. Schon jetzt werden große KI-Sprachmodelle von Cyberkriminellen bevorzugt dafür eingesetzt, Phishing-Nachrichten sowohl textlich als auch bildlich und stimmlich authentischer zu gestalten und damit die Erfolgsaussichten zu erhöhen. Auch Deepfakes werden in Zukunft eine größere Rolle spielen, sodass man in absehbarer Zeit nicht mehr sicher sein kann, ob man in Online-Meetings mit der realen Person, einem Angreifer oder sogar dem Avatar eines Chatbots spricht.[13] Ein Schreckensszenario, auf das sich Unternehmen schon heute einstellen müssen.

66%

aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34% Erpressungsmails
32% Betrugsmails

84%

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

[12] *TÜV, Cybersecurity Studie 2023*

[13] *Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2023*

Zwischenfazit

Die IT-Sicherheitslage deutscher Unternehmen ist zweifelsohne prekär, aber noch lange nicht aussichtslos. Denn auch wenn sich die cyberkriminelle Szene stetig weiterentwickelt und neue Taktiken entwirft, um insbesondere Modern-Work-Initiativen wie die Digitalisierung und Flexibilisierung des Arbeitsplatzes zu ihrem schändlichen Vorteil zu nutzen, so gibt es doch immer noch die gute Seite, die als Schutzschild fungiert und sowohl das Unternehmen als auch seine Anwender vor einem möglichen Schaden bewahrt.

Die Rede ist zum einen von smarten Köpfen, die sich die IT-Sicherheit auf die Fahnen geschrieben haben und strategisch vorangehen, um im Cyber War als Sieger hervorzugehen. Die Rede ist aber auch von intelligenten Technologien und Lösungen, die der gleichen Mission dienen, bereits am Markt verfügbar sind und nur genutzt werden müssen. Das Ziel muss es sein, gerade im Digital-Workspace-Umfeld, aber auch darüber hinaus, die eigene Cyberresilienz zu stärken – und das möglichst schnell, um handlungsfähig zu bleiben. Prävention ist hier das A und O, denn auch im Security-Kontext gilt:

Vorbeugen ist besser als heilen.

Cyberresilienz ist das Gebot der Stunde.

3/ Zero Trust. Vertraue niemandem.

„Vertrauen ist gut, Kontrolle ist besser." – auch wenn dieses Sprichwort gerade im Hinblick auf Modern-Work-Initiativen etwas aus der Zeit gefallen zu sein scheint, so ist es im Security-Kontext aktueller denn je. Denn die Kernbotschaft beschreibt nichts anderes als das Leitprinzip, mit dem sich ein innovatives Sicherheitskonzept über die letzten Jahre in die Herzen von Cybersecurity-Experten gespielt und erfolgreich etabliert hat: Zero Trust. Doch was steckt eigentlich hinter Zero Trust? Und wie lässt sich dieser Ansatz nutzen, um den Digital Workspace abzusichern? Aufschluss darüber liefern dieses und das nächste Kapitel.

Beginnen wir langsam: Generell ist Zero Trust ein herstellerunabhängiges Modell, das den Vertrauensgrundsatz neu denkt. Es basiert auf dem Prinzip, dass kein Nutzer und auch kein Gerät – weder innerhalb noch außerhalb eines Unternehmensnetzwerks – einen unkontrollierten Zugriff auf Daten oder Services erhalten soll.

Das wiederum bedeutet, dass es keine Endgeräte oder Schnittstellen mehr gibt, die von Grund auf vertrauenswürdig sind. Auch eine statische Zuordnung in sichere und unsichere Netzwerksegmente existiert nicht mehr. Stattdessen wird dynamisch anhand einer definierten und anschließend permanent überwachten Security Policy entschieden, ob Nutzer und Geräte (= Entitäten) als vertrauenswürdig gelten.

Die Prinzipien von Zero Trust

1. Aus dem fehlenden impliziten Vertrauen folgt, dass jede Entität sich authentisieren und anschließend autorisiert werden muss, um Zugriff auf Ressourcen zu erhalten. Dabei ist vor allem eine starke Authentifizierung entscheidend.

Never trust, always verify.

2. Das Prinzip der minimalen Rechte bedeutet, dass nur die Entitäten Zugriff erhalten, die auch Zugriff benötigen. Dies bedingt, dass Ressourcen in möglichst kleine Einheiten unterteilt und Berechtigungen möglichst feingranular vergeben werden müssen. Der kleinere Radius beschränkt im Fall eines böswilligen Zugriffs den unkontrollierten Abfluss oder die Manipulation von Daten und eine laterale Ausbreitung.

3. Nicht nur das externe, sondern auch das interne Netz wird fortwährend als unsicher erachtet und das erteilte Vertrauen nie dauerhaft gewährt. Auf Basis von dynamischen Zugriffsrichtlinien, kontinuierlicher Überwachung und Risikoanalysen wird das Vertrauen fortwährend bewertet und über Zugriffe jeweils neu entschieden.

Wichtig ist, dass Zero Trust keinen definierten Standard darstellt, sondern vielmehr als Architekturdesign-Paradigma zu verstehen ist, aus dessen Leitprinzipien bedarfsgerechte Gegen- und Härtungsmaßnahmen zum Schutz der IT-Infrastruktur abgeleitet werden können. Im Fokus steht die Sicherstellung der Datenintegrität und -vertraulichkeit, um sowohl die Resilienz der Daten, aber auch die der davon abhängigen Geschäftsprozesse einer Organisation zu steigern.

Darum ist Zero Trust so wichtig

Geänderte Struktur von Firmennetzwerken
Der Aufbau von Unternehmensnetzwerken hat sich in den vergangenen Jahrzehnten enorm verändert. Daten und Anwendungen, die einst auf einem zentralen Server lagerten, sind heute durch etablierte Modelle wie Software as a Service (SaaS) oder Platform as a Service (PaaS) auf unzähligen Cloud-Plattformen verstreut. Und dank Microsoft 365 und Microsoft Entra ID (ehemals Azure AD) wandern sogar Kernfunktionen der Office- und Enterprise-Software zunehmend in die Cloud.

Moderne Arbeitswelt
Wir kommen mit dem privaten Notebook in die Firma oder loggen uns von zuhause über VPN ins Firmennetzwerk ein; wir teilen Dokumente über SharePoint mit Außenstehenden oder legen gleich selbst einen Gast-Account in Teams für Partner und Dienstleister an: Die Art und Weise, wie wir heute arbeiten, führt zwar nachweislich zu mehr Produktivität, sorgt aber auch dafür, dass Daten und Systeme einem deutlich erhöhten Sicherheitsrisiko ausgesetzt sind.

Wachsende Cyberbedrohungen
Die Methoden der Cyberkriminellen werden immer ausgefeilter. Gleichzeitig bietet ihnen der Wechsel in die Cloud und die Dezentralisierung von Unternehmensnetzwerken eine sehr große Angriffsfläche. Setzt man unter diesen Voraussetzungen auf eine klassische Sicherheitsstrategie, die das eigene Netzwerk als geschützten Raum betrachtet, haben Angreifer bei Überwindung dieser Barriere freies Spiel und können auf fast alle Daten und Systeme zugreifen. Durch interne Absperrungen und Kontrollen, wie sie Zero Trust vorsieht, lässt sich genau das verhindern.

4/ Workspace Security.
Ansatzpunkte zur Optimierung.

Die Theorie hinter Zero Trust ist eine Sache, das Implementieren eine ganz andere. Spannend ist also die Frage, wie sich eine wirksame Zero-Trust-Architektur rund um den digitalen Arbeitsplatz realisieren lässt. Welche Bereiche gilt es beim Digital Workspace konkret zu betrachten? Welche Maßnahmen, Technologien und Lösungen spielen eine Rolle und sind aus Expertensicht zudem besonders empfehlenswert? **So viel vorweg: Die eine Zero-Trust-Lösung gibt es nicht.**

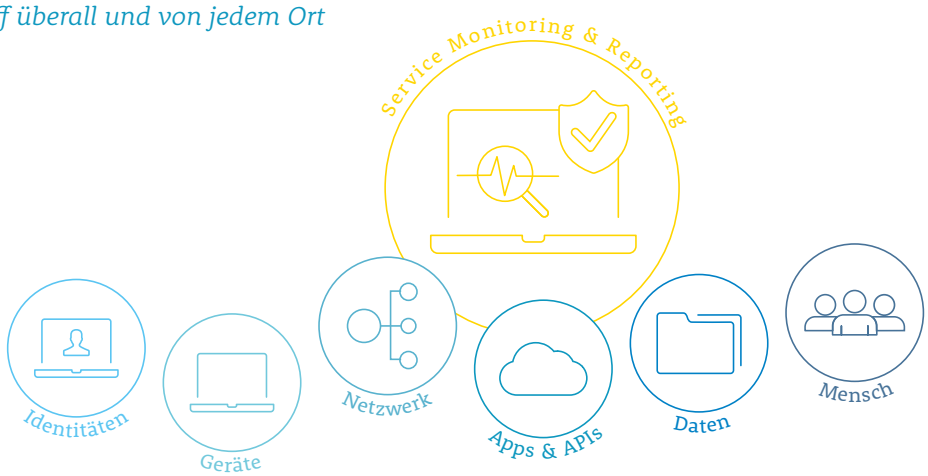
Entscheidet man sich für Zero Trust, entscheidet man sich für einen ganzheitlichen Ansatz, der eine Vielzahl verschiedener Schutzmaßnahmen und Best Practices vorsieht. Diese lassen sich insgesamt sechs themenspezifischen Säulen zuordnen, die durch eine an die Organisation angepasste Zero-Trust-Architektur ineinandergreifen. Dennoch kann jede Säule zunächst unabhängig von den anderen weiterentwickelt werden. Auf diese Weise gelingt eine schrittweise Integration der Zero-Trust-Prinzipien in Bestandsumgebungen, was sowohl die personellen als auch die finanziellen Ressourcen schont.

Oberstes Ziel sollte jedoch immer bleiben, jeder der sechs Säulen seine volle Aufmerksamkeit zu widmen. Denn nur durch eine kontinuierliche Optimierung aller Bereiche und das effiziente Zusammenspiel dieser lässt sich ein wirkungsvolles Schutzschild aufbauen, an dem sich Angreifer buchstäblich die Zähne ausbeißen.

Eine ganzheitliche Umsetzung der Zero-Trust-Prinzipien in allen sechs Bereichen der IT-Infrastruktur ist wichtig. Im Kontext der Workspace Security, die als Teil einer gesamtheitlichen Zero-Trust-Strategie verstanden werden kann, kommen allerdings nur fünf von ihnen wirklich zum Tragen: Netzwerk, Identitäten, Geräte, Apps und Daten. Vor diesem Hintergrund wird im Folgenden bewusst auf das Thema Infrastructure Security verzichtet. An dessen Stelle rückt stattdessen eine Komponente, die gerade in Bezug auf den digitalen Arbeitsplatz eine sicherheitsrelevante Hauptrolle spielt: Der Mensch.

Menschen, Prozesse, Technologien

Datenzugriff überall und von jedem Ort



// Identity Security

Geschäftsprozesse werden digitaler, Arbeitsmodelle dezentraler. Und mit dieser Entwicklung wächst die Gefahr durch Cyberattacken mit all ihren dramatischen Folgen. Dabei ist zu beobachten, dass es Angreifern zunehmend darum geht, Identitäten zu stehlen, um auf diesem Wege an Berechtigungen zu kommen und sich frei im Unternehmensnetzwerk bewegen zu können. Entsprechende Angriffsmethoden wie Phishing, Passwortdiebstahl und Privilege Escalation sind en vogue – und der Erfolg gibt ihnen Recht.

Vor diesem Hintergrund sind Unternehmen heute mehr denn je gefordert, ihre digitalen Identitäten vor Raub und Missbrauch zu schützen. Und Identity Security ist der effizienteste Ansatz, dies zu tun. Konkret geht es dabei um die Kreation unverwechselbarer digitaler Identitäten, indem ihnen spezifische Attribute wie zum Beispiel Login-Daten, E-Mail-Adresse oder ein Sicherheitstoken zugewiesen werden. Zusätzlich findet hier das Prinzip des geringsten Privilegs (PoLP Principle of Least Privilege) Anwendung, das dafür Sorge trägt, dass Nutzer nur so viele Rechte bekommen, wie sie tatsächlich benötigen.

Der dahinterstehende Gedanke lautet, dass jeder Anwender ein potenzieller Angriffsvektor sein kann. Ziel ist es, dieses Risiko mit Tätigkeiten, die unter dem Begriff Identity & Access Management (IAM) zusammengefasst sind, zu reduzieren. Beispiele hierfür sind u. a.:

> die Entwicklung von Rollen- und Rechtekonzepten
> die Definition von Attributen zur Erstellung von Richtlinien
> die Einrichtung sicherer Service-Zugriffe inklusive der Überwachungs- und Protokollsysteme
> die Bestimmung von Authentifizierungsmethoden wie Single Sign-On (SSO) oder Multi-Faktor-Authentifizierung (MFA)
> die kontinuierliche Überwachung und Analyse von Benutzerverhalten und das Aufspüren kompromittierter Identitäten

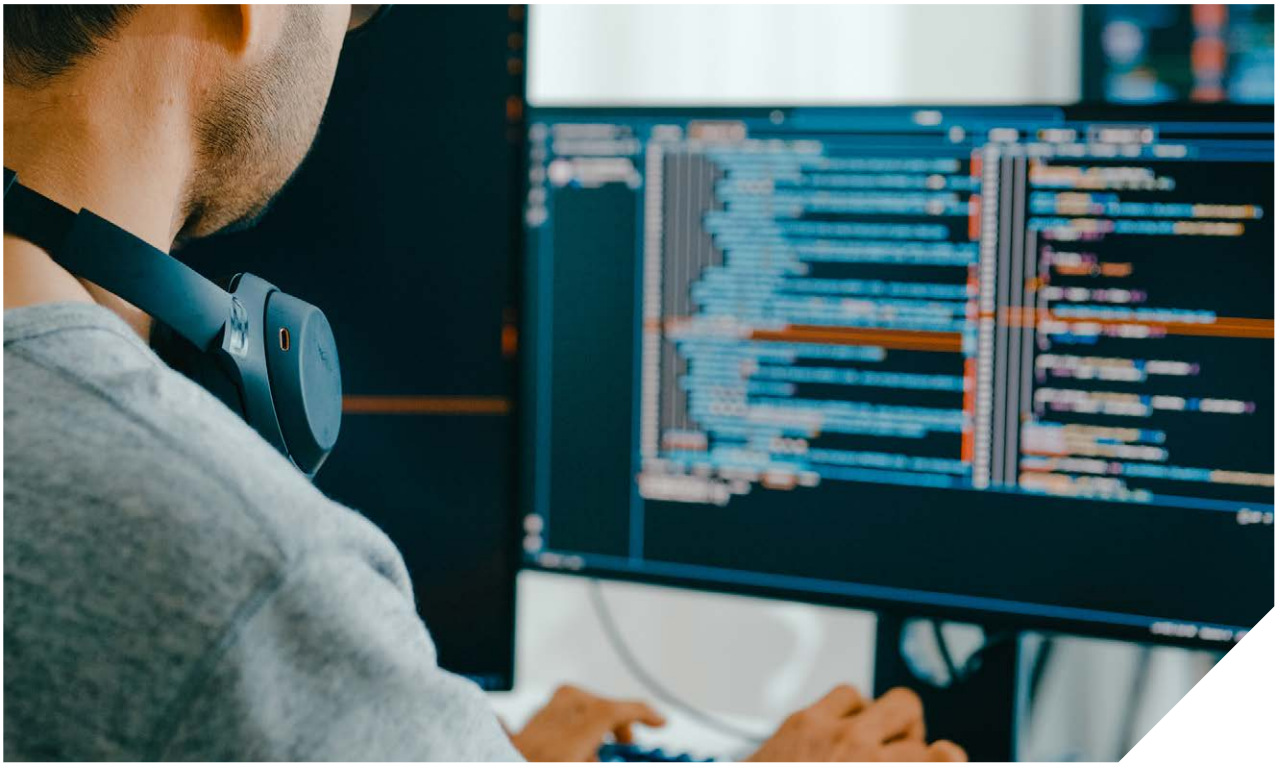
Folglich geht Identity Security weit über eine einfache Berechtigungsverwaltung hinaus. Es handelt sich vielmehr um einen ganzheitlichen Ansatz, der das fragliche Netzwerk und die Anwender gleichermaßen betrachtet und verschiedenste Maßnahmen berücksichtigt, die – ob einzeln oder im Zusammenspiel – zur Gewährleistung des Identitätsschutzes beitragen.

Relevante Themen

> Conditional Access
> Contextual Monitoring
> E-Mail-Security
> Identity & Access Management (IAM)
> Identity Threat Detection & Response
> Multi-Faktor-Authentifizierung (MFA)
> Passwordless Authentication
> PAW/AD-Tiering
> Privileged Access Management (PAM)
> Privileged Identity Management (PIM)
> Single Sign-On
> User/Device Risk Score

Relevante Anbieter

> BeyondTrust, Cisco, Delinea, Exabeam, Fortinet, IBM, Imprivata (Ogitix), Microsoft, Okta, Omada, Proofpoint, Recorded Future, RSA, SentinelOne, Thales



Das kann hochkomplex sein, muss es aber nicht. Denn Unternehmen können heute auf eine Vielzahl unterschiedlicher Lösungen zurückgreifen, die sie bei der Absicherung ihrer Identitäten unterstützen. So reicht das Angebot von einzelnen E-Mail-Security- und Authentifizierungslösungen über dedizierte Produkte zum Management privilegierter Zugriffe bis hin zu umfassenden IAM-Systemen, mit deren Hilfe Unternehmen automatisiert Konten, Rollen und Berechtigungen für alle Anwendungen, Systeme, Daten und Cloud-Dienste verwalten können. Besonders hilfreich sind in diesem Zusammenhang IAM-Lösungen, die mit KI- oder Machine-Learning-Funktionalitäten ausgestattet sind und es dadurch ermöglichen, dem richtigen Benutzer während des gesamten Mitarbeiter-Lebenszyklus den richtigen Zugriff zu gewähren.

Sie sehen, Identity Security ist essenziell. Und die Möglichkeiten, diese aufzubauen, sind vielfältig. Wichtig ist, damit anzufangen und die Maßnahmen so sukzessive zu erweitern, dass am Ende ein umfassender Identitätsschutz gewährleistet ist. Damit legen Sie die Schwelle für eine Vielzahl von Cyberangriffen von Vornherein maximal hoch, wodurch Ihr Unternehmen zumindest in diesem Bereich hinreichend abgesichert ist.

Use Case I:
Enterprise Single Sign-On im Gesundheitswesen

Geschwindigkeit kann Leben retten – und vor diesem Hintergrund sind Kliniken gefordert, ihre alltäglichen Abläufe immer weiter zu beschleunigen. Die Optimierung des klinikweiten Authentifizierungsmanagements ist in diesem Zusammenhang ein bedeutender Hebel, den es unbedingt zu nutzen gilt. Und am besten gelingt das mit der Einführung einer SSO-Lösung, die im Idealfall trotz eines erhöhten Sicherheitsniveaus eine „No-Click-Access"-Authentifizierung des Klinikpersonals ermöglicht und gleichzeitig die Einhaltung von Datenschutz- und Informationssicherheitsstandards unterstützt. Dabei geht eine moderne SSO-Lösung heute weit über die reine einmalige Passworteingabe als Authentifizierungsmethode hinaus. Es kann vielmehr aus vier Faktoren gewählt werden, die allesamt eine starke Authentifizierung gewährleisten. Dazu zählen vereinfacht gesagt etwas, das man weiß (eine persönliche PIN oder ein vertrauter Begriff), etwas, das man besitzt (Sicherheitstoken oder Zutrittskarte), etwas, worin man einzigartig ist (eindeutiges persönliches Merkmal, z.B. ein Fingerabdruck) oder ein Ort, an dem man sich befindet (Netzwerk, LAN/WAN).

Use Case II:
Der Onboarding-Prozess

Starten neue Mitarbeitende im Unternehmen, ist es der erste Eindruck, der zählt! Der Onboarding-Prozess wird damit zu einem bedeutenden Imagefaktor, der angesichts des bestehenden Fachkräftemangels nicht zu unterschätzen ist. Doch wie lässt sich der immer komplexer werdende Prozess aus IT- und Anwendersicht heute möglichst einfach und sicher gestalten? Die Lösung lautet IAM. Mit IAM lässt sich sicherstellen, dass der neue Mitarbeiter zu Arbeitsbeginn direkt einsatzfähig ist, ohne erst auf bestimmte Zugänge zu Applikationen, Verzeichnissen und Dokumenten warten zu müssen. Der Prozess kann dabei weitestgehend automatisiert erfolgen, indem Zugriffsrechte anhand definierter Rollen zugewiesen werden können.

Kurz & knapp:

Identity & Access Management

Identity & Access Management (IAM) steht für einen Organisationsprozess, der sich mit der Administration von User-Accounts und Applikationen befasst. Ziel ist es, dadurch Unternehmen eine effektive Verwaltung von Zugriffsrechten und Benutzeridentitäten zu ermöglichen. Dabei bildet IAM den Identity Lifecycle vollumfänglich ab und nutzt integrierte Prozesse, Workflows und Rollen, um jeder Identität ausschließlich die Systemzugänge zuzuweisen, die für die Ausführung der Aufgabe notwendig sind. Auf diese Weise lässt sich die Anzahl ungenutzter Benutzer-Accounts und Systemberechtigungen minimieren, wodurch die Bedrohung durch Cyberkriminalität sinkt.

Schlagkräftige Argumente für IAM

Verbesserung der IT-Sicherheit
Ein funktionierendes IAM minimiert das Risiko sozialer Attacken, indem es sicherstellt, dass jeder Benutzer nur die Berechtigungen hat, die er für die Ausführung seiner Tätigkeiten benötigt. Zusätzlich gewährleistet das Implementieren eines Rezertifizierungsprozesses, dass auch bei wechselnden Gegebenheiten die Nutzerberechtigungen im Unternehmen permanent nachgehalten werden.

Sichere Authentifizierungsmethoden
Laut einer Studie des renommierten Herstellers Yubico verbringen Mitarbeitende etwa 11 Stunden im Jahr mit der Verwaltung ihrer Zugänge und Passwörter. Außerdem verwenden durchschnittlich 51 Prozent der Befragten das gleiche Passwort für unterschiedliche Accounts, wodurch die alleinige Passwortauthentifizierung zunehmend als unsicher bewertet wird. IAM schafft dem Abhilfe, indem es Verfahren wie Single Sign-On und passwortlose Authentifizierungsmethoden nutzt.

Einhaltung von Compliance-Vorgaben
Unternehmen stehen in der Pflicht, bestimmte Sicherheitsstandards einzuhalten. IAM unterstützt bei der Einhaltung gesetzlicher und branchenspezifischer Anforderungen und hilft dabei, potenzielle Sanktionen zu vermeiden.

Kostenreduktion
Die Einführung einer IAM-Lösung ist zu Beginn mit Investitionen verbunden, die sich jedoch schnell bezahlt machen. Denn dank IAM können viele manuelle Tätigkeiten automatisiert werden, wodurch in den Bereichen Helpdesk, Genehmigung von Zugriffsrechten, Audit und Compliance bis zu 70 Prozent eingespart werden können. Darüber hinaus werden die Mitarbeitenden befähigt, mithilfe des Self-Services Standardtätigkeiten anzustoßen, die automatisiert und daher zeitnah umgesetzt werden.

Bad: Password	**Good:** Password and ...	**Better:** Password and ...	**Best:** Passwordless
123456 qwerty password iloveyou password1	SMS Voice	Authenticator (Push Notification) Software Tokens OTP Hardware Tokens OTP	Windows Hello Authenticator (Phone Sign-in) FIDO2 security key

// Endpoint Security

Von Desktops und Laptops über Smartphones und Tablets bis hin zu IoT-Geräten – ohne Endgeräte geht in der heutigen digitalen Geschäftswelt nichts mehr. Allerdings stellen sie auch erhebliche Angriffsvektoren dar, was ihre Absicherung umso wichtiger macht. In diesem Abschnitt erfahren Sie, wie Sie Ihre Gerätesicherheit unter Berücksichtigung der Zero-Trust-Prinzipien auf ein fortschrittliches Niveau heben können – und das alles unter Verwendung bereits vorhandener Technologien.

Eines vorneweg: Spricht man von einer sicheren Verwaltung von Endgeräten bzw. Endpunkten, so schließt das alle Devices ein, die auf interne Daten zugreifen. Dies umfasst neben unternehmenseigenen und privaten Endgeräten auch IoT-Geräte sowie sämtliche Anwendungen, die hierauf laufen. Daher ist es nicht überraschend, dass auch bei Endgeräten der zentrale Zero-Trust-Sicherheitsgedanke gilt: Vertraue niemanden, verifiziere alles.

Das Herzstück der Endgerätesicherheit ist das Prinzip der ständigen Wachsamkeit. Dahinter steckt der Gedanke, dass Bedrohungen auch von innen kommen können und zudem in der Lage sind, sich schnell anzupassen. Um diese Risiken zu minimieren, empfiehlt sich der Einsatz sogenannter EDR-Lösungen (kurz für: Endpoint Detection and Response). EDR geht dabei weit über herkömmliche Antiviren-Software hinaus, indem es Endpunkte kontinuierlich auf verdächtige Aktivitäten überwacht. Erkennt die EDR-Lösung eine potenzielle Gefahr, reagiert sie in Echtzeit, isoliert das Gerät oder ergreift alle notwendigen Maßnahmen, um die Bedrohung zu neutralisieren.

Um einen umfassenden Endgeräteschutz zu gewährleisten, sollte das proaktive Monitoring um eine weitere, äußerst wichtige Komponente ergänzt werden: das Unified Endpoint Management (UEM). UEM-Lösungen gelten als fester Bestandteil des Zero-Trust-Modells, erlauben sie doch das Management ausnahmslos aller im Unternehmen registrierten Endgeräte von zentraler Stelle. Dank ihnen ist es möglich, Sicherheitsrichtlinien für mobile Geräte unternehmensweit durchzusetzen, alle Geräte mit aktuellen Patches zu versorgen, die Verschlüsselung zu aktivieren sowie eine sichere Konfiguration zu realisieren. Des Weiteren kann mit ihrer Hilfe sichergestellt werden, dass ausschließlich berechtigte Geräte, Nutzer und Applikationen auf schützenswerte Daten zugreifen können. Dafür sorgen etablierte Funktionen wie Application Control, Conditional Access, Device Compliance oder Privilege Management, die heute in jeder modernen UEM-Lösung integriert sind.

Das Must-have: Patchmanagement

250.000 neue Schadsoftware-Varianten pro Tag treffen auf täglich knapp 70 neue Schwachstellen in Softwareprodukten[14]: Diese Erkenntnis des BSI lässt aufhorchen und gibt Unternehmen gleichzeitig einen Hinweis darauf, wie wichtig es ist, die IT-Systeme mithilfe eines soliden Patchmanagements zu schützen. Denn Schwachstellen in Software – seien es Betriebssysteme, Applikationen oder die Firmware diverser Produktions- und Überwachungssysteme – sind noch immer das wichtigste Einfallstor für Schadprogramme. Und werden Patches nicht regelmäßig in die Systeme eingespielt, wozu auch jegliche Endgeräte, Drucker und Switches gehören, bleiben diese offen und können umfangreich ausgenutzt werden. Damit avanciert das Patchmanagement zur zentralen Säule eines sicheren IT-Betriebs, die wirksam vor großem Schaden bewahrt.

Ausführlichere Informationen zum Thema Patchmanagement finden Sie auf Seite 36.

Immer wichtiger: Kontextbasierte Sicherheit

Nutzen Organisationen eine UEM- in Kombination mit einer EDR-Lösung, haben sie bereits die grundlegenden Weichen für die Sicherheit ihrer Endgeräte gelegt. Doch es geht bekanntlich immer noch mehr: Gerade mit Blick auf den digitalen Arbeitsplatz und der damit verbundenen flexiblen Arbeitsweise der Mitarbeitenden ist es unabdingbar, auch den Kontext wie z. B. den Ort des Zugriffs oder den Status der Sicherheitseinstellungen des zugreifenden Endgeräts in die Gleichung miteinzubeziehen. Hierzu werden vor dem versuchten Zugriff alle Kontextinformationen, die aus Sicht der Unternehmens-IT relevant sind, automatisch und in Echtzeit ermittelt und geprüft – und das kontinuierlich während der laufenden Session. Entsprechen Parameter nicht den IT-seitigen Anforderungen in puncto Sicherheit, Compliance und Regulatorik, werden dem Anwender der Zugang zu den Unternehmensdaten verwehrt und unter Umständen sogar Remote-Anwendungen sofort gesperrt.

[14] *Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2023*

Die Sicherheit der Endgeräte gehört zu den wichtigsten Eckpfeilern für eine robuste Cybersecurity-Strategie. Daher sollten Sie lieber heute als morgen damit beginnen, geeignete Strategien und Technologien zu implementieren, die dazu beitragen, Ihre digitale Verteidigungslinie zu stärken. Dabei zählt: Viel hilft viel! Denn nur durch das Zusammenspiel verschiedener, aufeinander abgestimmter Maßnahmen stellen Sie sicher, dass Ihre Endgeräte zu verlässlichen Partnern werden.

Relevante Themen

- Application Allowlisting
- Conditional Access
- Contextual Security
- Device Control
- Device Encryption
- Endpoint Detection & Response (EDR)
- Extended Detection & Response (XDR)
- Modern Device Management
- Patchmanagement
- Unified Endpoint Management (UEM)

Relevante Anbieter

- Check Point, deviceTRUST, Fortinet, Ivanti, Jamf, Matrix42, Microsoft, Omnissa, Palo Alto, SentinelOne, TrendMicro

Endpoint Security ohne Kompromisse

Unified Endpoint Management

An Unified Endpoint Management (UEM) führt in diesen Zeiten kein Weg mehr vorbei. Alle Endgeräte sind heutzutage mit dem Internet verbunden und sie alle stellen dadurch fortwährend einen potenziellen Angriffsvektor dar. Diese Tatsache macht UEM zur Pflicht für jedes Unternehmen, das seine Systeme und Daten zu jeder Zeit in sicheren Gefilden wissen möchte.

Schlagkräftige Argumente für UEM

Fortwährende Prüfung der Device Compliance
Anhand vordefinierter Eigenschaften und Sensoren wird ein Endgerät als ‚sicher' oder ‚unsicher' eingestuft. Entspricht das Gerät nicht den gesetzten Vorgaben, kann der Zugriff auf Unternehmensdaten und -anwendungen so lange verwehrt werden, bis der gewünschte Status (der sog. Desired State) wiederhergestellt ist. Zudem sind die Ermittlung und Einbeziehung des Risk Scores sowohl vom Gerät als auch vom Benutzer möglich, um den Zugriff auf Anwendungen und Daten zu reglementieren.

Anwendung und Umsetzung von Sicherheitsrichtlinien
Von der Mehrfaktorauthentifizierung über die Kennwortkomplexität bis hin zu Datenverschlüsselungsmethoden – Administratoren können mit einem einzigen Tool einheitliche Richtlinien und Baselines für alle Geräte festlegen und unternehmensweit ausrollen.

Push-Bereitstellung von Patches und Updates
UEM kann Endpunkte auf Schwachstellen in der Software, Firmware oder im Betriebssystem prüfen und bei Bedarf automatisch Patches und Updates per Push-Operation installieren.

Identifikation und Behebung von Sicherheitsrisiken
Dank der Integration von User and Entity Behavior Analytics (UEBA), Endpoint Detection and Response (EDR) und weiterer Sicherheitstechnologien kann UEM dazu beitragen, verdächtiges Geräteverhalten zu identifizieren und bei Bedarf Maßnahmen zu ergreifen, um potenziellen Sicherheitsrisiken entgegenzuwirken.

Remote-Sperrung gestohlener oder verloren gegangener Geräte
Administratoren haben die Möglichkeit, verloren gegangene, gestohlene oder stillgelegte Geräte zu lokalisieren, zu bereinigen, zu sperren und/oder zurückzusetzen. Auf diese Weise wird der unbefugte Zugriff auf das Netz vermieden und gleichzeitig verhindert, dass die vertraulichen Daten auf dem Gerät in die falschen Hände geraten.

// Network Security

Mit der zunehmenden Mobilität der Mitarbeitenden und dem vermehrten Einsatz von Cloud-Anwendungen verlieren herkömmliche Modelle für die Netzwerksicherheit drastisch an Relevanz. Ihr Wirkungsgrad ist eingeschränkt; es fehlt an Agilität, Flexibilität und fortschrittlichen Schutzfunktionen, die angesichts der Bedrohungslage heutzutage unabdingbar sind. Moderne Organisationen sind also gefordert, schnellstmöglich zu handeln und besser heute als morgen eine Alternative zu finden, die keinerlei Kompromisse bei der Absicherung des Netzwerks zulässt. Wir zeigen Ihnen, welche das sein kann – doch beginnen wir von vorne …

Um ihre IT-Systeme zu schützen, setzen auch heute noch viele Unternehmen auf Sicherheitsarchitekturen nach dem Prinzip „Festung mit Burggraben", die auf Perimeter-Firewalls beruhen. Hierbei kommen eine Reihe von Verteidigungslinien zum Einsatz, die verhindern sollen, dass Cyberkriminelle den Perimeter durchbrechen. Wird eine Verteidigungslinie überwunden, wartet dahinter bereits die nächste.

Diese Strategie funktioniert aber nur so lange, bis Cloud-Technologien und mit ihnen dezentrale Arbeitsmodelle Einzug ins Unternehmen halten. Denn diese Entwicklungen sorgen zum einen dafür, dass sich der Netzwerk-Traffic nicht mehr in erster Linie durch eine lokale Netzwerkinfrastruktur, sondern vielmehr quer durch das Internet bewegt. Und zum anderen steigt durch die wachsende Anzahl an Remote-Usern stetig die Gefahr, auch innerhalb des Netzwerkes angegriffen zu werden. Für beides sind Legacy-Lösungen nicht optimal aufgestellt. Was es stattdessen braucht, sind Sicherheitsansätze, die u. a. mehr Agilität, eine bessere und zuverlässigere Netzwerkleistung sowie mehr Transparenz und Kontrolle in heterogenen IT-Umgebungen versprechen.

In diesem Zusammenhang hat sich über die letzten Jahre das SASE-Modell (kurz für: Secure Access Service Edge) bewährt – ein Sicherheitsframework, das SD-WAN-Funktionalität und Zero-Trust-Sicherheitslösungen in einer cloudbasierten Plattform zusammenführt, die wiederum Benutzer, Systeme, Endpunkte und Remote-Netzwerke auf sichere Weise mit Apps und Ressourcen verbindet. Konkret umfasst SASE dabei sechs zentrale Technologien:

- **Software-Defined Wide Area Network (SD-WAN)**
  Hierbei handelt es sich um eine virtuelle WAN-Architektur, die den Datenverkehr auf nahtlose, sichere und effiziente Weise zu/von entfernten Orten leitet und dabei eine zentralisierte Richtlinienkontrolle und -verwaltung nutzt.

- **Secure Web Gateway (SWG)**
  Ein SWG überwacht den Web-Traffic in Echtzeit, filtert bösartige Inhalte und Anwendungen heraus, implementiert Sicherheitsrichtlinien und ermöglicht die sichere Nutzung des Internets durch Benutzer unabhängig von ihrem Standort oder Endgerät. Es schützt Organisationen vor Bedrohungen wie Malware, Phishing und Datenverlust, während es die Produktivität der Benutzer durch Kontrolle und Optimierung des Web-Traffics unterstützt.

- **Cloud Access Security Broker (CASB)**
  Die SaaS-Anwendung fungiert als Sicherheitskontrolle zwischen lokalen Netzwerken und cloudbasierten Anwendungen und setzt Datensicherheitsrichtlinien durch. Verfahren für Prävention, Überwachung und Risikominderung werden kombiniert, um Unternehmensdaten zu schützen.

- **Firewall as a Service (FWaaS)**
  Mit FWaaS verlagert sich der Firewallschutz vom traditionellen Netzwerkperimeter in die Cloud. Dadurch können sich Remote-User sicher mit dem Unternehmensnetzwerk verbinden und Unternehmen einheitliche Sicherheitsrichtlinien implementieren, die über ihre geografische Reichweite hinausgehen.

- **Zero Trust Network Access (ZTNA)**
  Bei ZTNA handelt es sich um verschiedene konsolidierte, cloudbasierte Technologien in einem Framework, in dem keine Verbindung automatisch als vertrauenswürdig eingestuft wird. Der Zugriff wird allen Benutzern, Geräten und Anwendungen nach dem Erforderlichkeitsprinzip auf Basis der geringstmöglichen Berechtigungen gewährt. Folglich müssen alle Benutzer authentifiziert, autorisiert und laufend überprüft werden, bevor sie Zugang zu unternehmensinternen Anwendungen und Daten erhalten.

- **Zentrale und einheitliche Verwaltung**
  Durch die Verwaltung des gesamten Funktionsumfangs über eine einzige Konsole können viele Herausforderungen rund um Änderungskontrolle, Patchmanagement, Koordinierung von Ausfallzeiten und Richtlinienverwaltung vermieden werden. Richtlinien lassen sich unternehmensweit unabhängig vom Standort der User konsistent durchsetzen.

Während sich klassische Network-Security-Maßnahmen ausschließlich auf externe Zugriffe und Netzwerkverkehr beschränken, geht der Zero-Trust-Ansatz tiefer und misstraut grundsätzlich jedem Vorgang und Nutzer – egal ob intern oder extern. Das ist angesichts der neuen Herausforderungen auch nur richtig und wird dringend empfohlen. Entsprechend sollte jedes Unternehmen, das sein Netzwerk umfassend vor Bedrohungen geschützt wissen will und gleichzeitig seine digitale Transformation voranbringen und Mobil- oder Hybridarbeit unterstützen möchte, ein SASE-Framework implementieren.

Relevante Themen

- Cloud Access Security Broker (CASB)
- Data Encryption
- Network Access Control (NAC)
- Network Segmentation
- Remote Browser Isolation
- Secure Access Service Edge (SASE)
- Secure Internet Access (SIA)
- Security Services Edge (SSE)
- Zero Trust Network Access (ZTNA)

Relevante Anbieter

- Check Point, Cisco, Citrix, Fortinet, Ivanti, Microsoft, Netskope, Palo Alto, Vectra

Höchste Zeit für eine Ablösung

ZTNA schlägt VPN

Virtual Private Networks (VPNs) haben sich als Legacy-Lösung jahrelang bewährt, boten sie Unternehmen doch bis dato eine effektive Möglichkeit, ihren Remote-Benutzern über einen speziell eingerichteten Tunnel einen sicheren Zugriff auf das Unternehmensnetzwerk und die dort gehosteten Ressourcen zu gewähren. Mit dem Trend zu dezentralen Arbeitskonzepten zeigt sich jedoch immer mehr, dass VPNs an ihre Grenzen stoßen: Skalierungsprobleme verbunden mit einem hohen Kosten- und Betriebsaufwand werden für Unternehmen zunehmend zu einer Herausforderung. Auch beeinträchtigt der Wechsel vieler Organisationen zu öffentlichen Cloud-Umgebungen sowohl die konsistente Durchsetzung von Sicherheitsrichtlinien für Remote-Mitarbeitende als auch die Qualität der Benutzererfahrung.

Das Hauptproblem ist damit aber noch nicht einmal benannt. Denn VPNs vergrößern die Angriffsfläche der betreffenden Organisationen erheblich. Jeder Benutzer oder jede Entität mit den richtigen Zugangsdaten kann sich in einem VPN anmelden und hat dann laterale Bewegungsfreiheit im gesamten Netzwerk. Mit anderen Worten: Sie können auf alle Ressourcen und Daten zugreifen, die das VPN eigentlich schützen soll. Angesichts der aktuellen Bedrohungslage und dem vermehrten Trend zu Social-Engineering-Angriffen ist diese Erkenntnis nicht wirklich beruhigend. Unternehmen sollten daher alles daran setzen, ihre bestehende VPN-Lösung perspektivisch durch eine bessere Alternative zu ersetzen.

Besser heißt in diesem Fall: Zero Trust Network Access (ZTNA). Denn im Gegensatz zu VPN setzt ZTNA zur Gewährleistung des sicheren User-Zugriffs das Prinzip der minimalen Rechtevergabe durch. Das bedeutet, dass die Vertrauenswürdigkeit von Usern und Entitäten nicht mehr allein durch die Überprüfung der Zugangsdaten verifiziert wird, sondern anhand erweiterter Kontextinformationen. Demzufolge werden Zugriffsanfragen nur genehmigt, wenn Benutzer, Identität, Gerät und Standort stimmig sind.

Als weiterer Vorteil kommt hinzu, dass ZTNA keinen Netzwerkzugang erlaubt. Stattdessen wird Nutzern durch sichere Direktverbindungen granularer Zugriff auf die jeweils benötigten Daten und Ressourcen gewährt. Dadurch haben Bedrohungsakteure keine Chance, sich lateral innerhalb des Netzwerks zu bewegen, selbst wenn es ihnen gelingt, sich Zugriff auf einzelne Ressourcen zu verschaffen. Durch den Direktzugriff in einem ZTNA-Framework lässt sich zudem eine erhebliche Verbesserung der Benutzererfahrung erzielen: Anwendungen sind schneller erreichbar, da Tunnel nicht mehr für das gesamte Gerät, sondern nur noch pro App aufgebaut werden müssen.

// Application Security

Von klassischen CRM- und ERP-Systemen über cloudbasierte Office- und Grafikprogramme bis hin zu kleinen mobilen Apps – heutzutage haben Unternehmen hunderte, wenn nicht gar tausende Business-Anwendungen im Einsatz, um ihre Geschäftsprozesse digital abzubilden. Wird man sich bewusst, dass mit diesen Anwendungen in der Regel auch unternehmenskritische Daten verarbeitet werden, auf die auch noch von intern und extern zugegriffen werden kann, so wird schnell deutlich: Der Schutz von Applikationen ist nicht verhandelbar.

Nun ist es im Hinblick auf die wachsende Komplexität moderner Anwendungen gar nicht so einfach, sie vor etwaigen Bedrohungen abzusichern. Doch es geht – und zwar sehr gut! –, wenn Sie sich von vornherein auf die zwei wichtigsten Handlungsfelder konzentrieren: Die Härtung der Anwendung selbst sowie den Aufbau eines Schutzschildes, das die Applikationen effizient und dauerhaft vor unbefugten Zugriffen schützt.

Um zu verstehen, wie eine Anwendung von innen heraus widerstandsfähiger gegen Angriffe gemacht werden kann, eignet sich der Vergleich mit einer Impfung. Impfungen gelten bis heute als effektivste Präventivmaßnahme, um die körpereigene Immunabwehr gegen Erreger zu aktivieren und somit Infektionskrankheiten zu vermeiden. Ganz ähnlich stellt es sich bei der Härtung von Anwendungen dar, denn auch hier gibt es hocheffiziente Schutzmaßnahmen. Die Rede ist von Vulnerability Management und Patchmanagement – ein Duo, das im Zusammenspiel wie kein anderes die inneren Abwehrkräfte stärkt.

- **Vulnerability Management,** auch bekannt als Schwachstellenmanagement, bezeichnet einen fortlaufenden Prozess, mit dessen Hilfe Sicherheitslücken in Systemen und in der auf diesen Systemen laufenden Software erkannt, bewertet, behandelt und gemeldet werden. Entsprechende Tools verfolgen hierbei aktuell einen kontextbezogenen, risikobasierten Ansatz, was es Unternehmen ermöglicht, die identifizierten Schwachstellen anhand ihrer Kritikalität zu priorisieren und eine schnelle Behebung einzuleiten.

- **Patchmanagement** übernimmt im Anschluss den imaginären Staffelstab aus dem Vulnerability Management und schließt die erkannten Schwachstellen durch das regelmäßige Einspielen sicherheitsrelevanter Updates (Patches). Was das Patchen so wichtig macht und warum eine Vernachlässigung nicht nur im Kontext der Anwendungssicherheit keine Option darstellen sollte, lesen Sie auf Seite 36.

Die Härtung der eingesetzten Applikationen ist das eine. Das andere ist, sie möglichst umfassend vor missbräuchlichen Zugriffen abzusichern. Auch hierfür gibt es verschiedenste Möglichkeiten, die je nach Unternehmensanforderungen einzeln oder in Kombination einen wirkungsvollen Schutz gewährleisten. Zu den wichtigsten von ihnen zählen der Einsatz von Mobile Application Management, Identity & Access Management und Conditional Access.

> **Mobile Application Management (MAM)** ist ein zentraler Bestandteil moderner UEM-Lösungen (siehe Seite 29). Durch das Isolieren von Firmendaten in einer verschlüsselten Sandbox und die granulare Kontrolle über Firmen-Applikationen sind diese auch bei privater Nutzung des Gerätes optimal geschützt. Des Weiteren sorgen Data-Loss-Prevention-Einstellungen dafür, dass ein Datenabfluss von gemanagten zu ungemanagten Apps unterbunden wird. Ein applikationsbasiertes VPN vereinfacht außerdem den Zugang zu Firmenressourcen, ohne das interne Netzwerk unnötig zu belasten, wodurch beispielsweise auch BYOD-Szenarien sicher und zuverlässig umgesetzt werden können.

> **Identity & Access Management (IAM)** befasst sich mit Konzeption und Umsetzung eines intelligenten Berechtigungsmanagements. Auf Seite 25 dieser Broschüre erfahren Sie, was genau dahintersteckt.

> **Conditional Access** („Bedingter Zugriff“) ist eine der wirksamsten Methoden, um Zugriffe auf interne Dienste oder Ressourcen Zero-Trust-konform zu steuern. Hierbei können Administratoren den Umfang des Zugriffs, den User auf Unternehmensapplikationen haben, feingranular kontrollieren – und zwar basierend auf dem Kontext, in dem sie versuchen, sich einzuloggen. Je nachdem, wie riskant ein Login-Versuch erscheint, können unterschiedliche Zugriffsvoraussetzungen definiert oder aber der Zugriff blockiert werden.

Anwendungen sind anfällig. Und je mehr Anwendungen ein Unternehmen nutzt, desto angreifbarer wird es. Vor diesem Hintergrund ist das frühzeitige Erkennen und Beheben von Schwachstellen und Sicherheitslücken das A und O für einen umfassenden Anwendungsschutz. Doch IT-Verantwortliche müssen darüber hinausgehen: Da die Techniken von Cyberkriminellen immer ausgefeilter werden, braucht es weitere moderne Sicherheitswerkzeuge, um ihnen einen oder idealerweise mehrere Schritte voraus zu sein. Die Etablierung einer intelligenten Zugriffsverwaltung kann hierbei für den nötigen Antrieb sorgen.

Relevante Themen

> App & Desktop-Virtualisierung
> Application Permissions
> Application Integrity
> Conditional Access
> Digital Employee Experience (DEX)
> Kontextbasierter Zugriff
> Mobile Application Management
> Patchmanagement
> Scan auf Anomalien
> Vulnerability Management

Relevante Anbieter

> deviceTRUST, Fortinet, Ivanti, Microsoft, Mondoo, Omnissa, Palo Alto, Pentera, SentinelOne, Tenable, TrendMicro, XM Cyber

Nur ‚Für', kein ‚Wider'
Patchmanagement

Das Patchmanagement gehört zu den zentralen Bausteinen im Kampf gegen Cyberangriffe. Und doch wird diese Aufgabe oftmals noch immer stiefmütterlich behandelt. „Zu mühsam", sagen die einen, „zu störanfällig" die anderen. Blickt man jedoch auf die aktuelle Sicherheitslage und betrachtet gleichzeitig das existierende Angebot an modernen Patchmanagement-Lösungen, so wird schnell klar, dass diese Aussagen nicht mehr als Ausrede herhalten können (und dürfen).

Dass Patchmanagement immer herausfordernder wird, ist unumstritten. Denn nicht nur die Zahl der von Unternehmen genutzten Anwendungen steigt stetig, sondern auch die Komplexität der zugrundeliegenden IT-Infrastruktur. Auf der anderen Seite gelingt es Cyberkriminellen, Angriffe zunehmend professioneller und schneller auszuführen und sich dabei länger unter dem Radar zu verstecken. Dies kann zu enormen Schäden führen, weshalb es wichtig ist, mit den heutigen Cybersicherheitsbedrohungen Schritt zu halten. Ein solides Patchmanagement, das in weiten Teilen auch schon automatisiert erfolgen kann, bietet hierfür den Grundpfeiler. Denn es hilft, auf plötzlich bekannt gewordene Sicherheitslücken in Windeseile zu reagieren.

Schlagkräftige Argumente für ein Patchmanagement

1. **IT-Sicherheit**
   Mehr als 2.000 neue Software-Schwachstellen pro Monat, davon 15 Prozent kritisch[15] – Angreifer wissen um die wachsende Zahl von Sicherheitslücken und nutzen diese präferiert für das Einschleusen ihrer Schadprogramme. Werden Patches nicht regelmäßig eingespielt, bleiben diese offen und können umfangreich ausgenutzt werden. Das Patchmanagement avanciert damit zur zentralen Säule, ohne die ein sicherer IT-Betrieb nicht zu gewährleisten ist.

2. **Compliance**
   Compliance beschreibt die Einhaltung von Gesetzen und Richtlinien eines Unternehmens durch Umsetzung von Vorgaben. Hierzu zählen branchenspezifische Vorgaben oder Standards wie z. B. die PCI DSS, unternehmensspezifische Vorgaben wie beispielsweise interne Verordnungen oder rechtliche Vorgaben wie die DSGVO. Diese Vorgaben können direkt oder indirekt ein Patchmanagement voraussetzen.

3. **Haftung der Geschäftsführung**
   Geschäftsführer sind im Rahmen ihrer Sorgfaltspflicht angehalten, die IT-Sicherheit des Unternehmens mithilfe eines funktionierenden Patchmanagements zum „Stand der Technik" zu gewährleisten. Ist kein angemessenes Patchmanagement aktiv und es kommt zu einem akuten IT-Sicherheitsvorfall aufgrund einer nicht gepatchten Schwachstelle, droht die persönliche Haftung des Geschäftsführers.

[15] *Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2023*

// Data Security

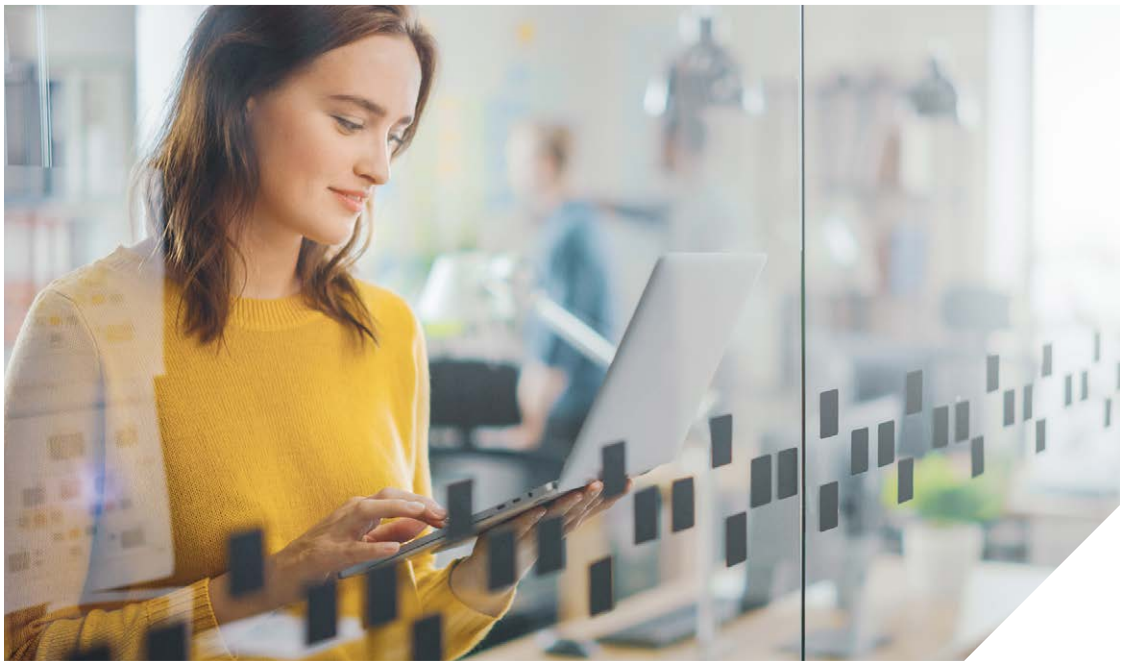
Datensicherheit ist das Herzstück von Zero Trust. Denn Daten – seien es personenbezogene Daten, sensible Gesundheits- oder Finanzinformationen oder geistiges Eigentum – sind das wertvollste Gut eines Unternehmens. Folglich haben es die meisten Angreifer genau darauf abgesehen, um größtmöglichen Schaden anzurichten. Die Gefahr durch Ransomware-Attacken und Datendiebstähle ist und bleibt also weiterhin groß und Unternehmen sind gefordert, ihr mit wirkungsvollen Sicherheitsstrategien zu begegnen.

Doch wo fängt man an? Und wann ist es genug? Generell gilt: Für Zero-Trust-Datensicherheit müssen Schutzmaßnahmen überall dort implementiert werden, wo Daten erfasst, verarbeitet, transportiert und gespeichert werden. Und nur durch das Zusammenspiel dieser Maßnahmen lässt sich eine starke verteidigungsfähige Architektur aufbauen, die den folgenden zwei Zielsetzungen dient: dem Schutz gegen Cyberangriffe und einer sicheren Datenhaltung. Ein Beginn lohnt sich also an allen Fronten und ein ‚genug' kann und wird es angesichts der Entwicklungen im Cybercrime-Markt so schnell nicht geben. Orientierung darüber, welche Sicherheitsmaßnahmen erforderlich sind, liefert das Zero-Trust-Modell selbst.

Als erstes geht es um die Erhöhung der Datenresilienz. Dies erfordert, dass alle Daten sowie der gesamte Datenverkehr verschlüsselt werden und unveränderliche Kopien der Daten existieren müssen, damit die Daten im Falle einer Katastrophe oder eines Angriffs besser geschützt und schnell wiederhergestellt werden können. Letzteres ist vor allem dadurch bedingt, dass auch immer häufiger Backup-Systeme und deren Datenspeicher ins Visier der Angreifer geraten. Denn schließlich sind Unternehmen bei einer Ransomware-Attacke eher bereit, auf Lösegeldforderungen einzugehen, wenn zusätzlich die Sicherungen betroffen sind. Um sich gegen diese erpresserischen Absichten zu schützen, müssen Unternehmen also auch ihr Backup gegen ungewollte Verschlüsselung absichern. Und das gelingt am besten mit unveränderlichen, redundanten Backups, die sich im Idealfall an physisch getrennten Orten befinden und mit minimalen Zugriffsrechten ausgestattet sind.

Ein weiterer wichtiger Aspekt zur Wahrung der Datenintegrität und -vertraulichkeit ist die Beschränkung des Zugriffs. Damit hier die Zero-Trust-Prinzipien greifen können, sollten Unternehmen im Vorfeld ihre sensiblen Daten mitsamt ihres Ablageorts identifizieren und nach Vertraulichkeitsstufe klassifizieren. Sind diese Hausaufgaben gemacht, lassen sich geeignete Maßnahmen implementieren, die sicherstellen, dass nur die Personen Zugang zu Daten erhalten, für die sie auch berechtigt sind. Multi-Faktor-Authentifizierung, granulare rollenbasierte Zugriffskontrolle (RBAC) oder privilegierte Accounts sind nur einige nennenswerte Methoden, die hierfür infrage kommen.

Als letztes sieht der Zero-Trust-Ansatz gezielte Maßnahmen im Bereich Erkennung und Analytik vor. Denn nur durch eine kontinuierliche Überwachung und Analyse aller Aktivitäten, die im Zusammenhang mit dem Datenzugriff stehen, sind Unternehmen in der Lage, Ransomware-Attacken oder Insider-Bedrohungen frühzeitig aufzuspüren. Besonders bewährt haben sich diesbezüglich Lösungen, die mit KI- oder ML-Modellen arbeiten und somit eine intelligente Datenüberwachung ermöglichen (siehe auch ‚Security Monitoring & Reporting', Seite 42).



Ein Zero-Trust-Ansatz beginnt mit dem Schutz Ihrer Daten. Daher empfehlen wir Ihnen, sich zuallererst dieser Aufgabe zu widmen, um im Anschluss weitere Sicherheitsebenen aufzubauen. So können Sie von Anfang an sicherstellen, dass ein Angreifer, der beispielsweise Perimeter-Kontrollen erfolgreich durchbrechen, eine Schwachstelle ausnutzen oder einen Insider bestechen konnte, am Ende an dem eingeschränkten Datenzugriff scheitert und folglich leer ausgeht.

Relevante Themen

- Backup
- Data Loss Prevention (DLP)
- Datenklassifizierung/-verschlüsselung
- Integrative Disaster Recovery (IDR)
- Sicheres Filesharing
- User and Entity Behavior Analytics

Relevante Anbieter

- IBM, Microsoft, Proofpoint, SEPPmail, Varonis

Kurz & knapp
Data Loss Prevention

Bei Data Loss Prevention (DLP) handelt es sich um eine Strategie und eine Reihe von Werkzeugen, die sicherstellen sollen, dass sensible Daten das Unternehmen nicht ohne die entsprechende Genehmigung verlassen. Hierbei übernehmen dedizierte DLP-Lösungen die Aufgabe, die Daten sowohl während der Übertragung als auch im Ruhezustand und bei der Verwendung zu identifizieren, zu überwachen und zu schützen, um dadurch Datenlecks, unbefugtem Datentransfer oder Insider-Bedrohungen wirksam entgegenzuwirken. Dies wird erreicht durch:

> Identifizierung sensibler Informationen: DLP-Lösungen klassifizieren Daten je nach ihrer Sensibilität. Beispielsweise werden Dokumente als vertraulich, öffentlich oder eingeschränkt gekennzeichnet.
> Überwachung der Daten: DLP-Tools verfolgen, wohin die Daten gehen, wer auf sie zugreift und wie sie verwendet werden. Wenn zum Beispiel ein Vertriebsmitarbeiter versucht, die gesamte Kundendatenbank auf einen USB-Stick herunterzuladen, würde ein DLP-Tool diese Aktion melden.
> Schutz von Daten: Wird eine potenzielle Bedrohung oder eine nicht autorisierte Aktion erkannt, können DLP-Lösungen die Aktivität blockieren, Sicherheitsteams alarmieren oder die Daten sogar in Echtzeit verschlüsseln.

DLP beschränkt sich jedoch nicht nur auf die lokale Datenlandschaft. Auch moderne Arbeitsumgebungen, in denen Cloud Computing und Remote-Arbeit eine wesentliche Rolle spielen, werden berücksichtigt. Entsprechend schützt DLP Daten über verschiedene Plattformen hinweg – ganz gleich, ob es sich um ein in einer Cloud-Speicherlösung gespeichertes Dokument oder eine über eine Instant-Messaging-Plattform gesendete Nachricht handelt.

Schlagkräftige Argumente für DLP

Schutz vor Datenschutzverletzungen und Datenleaks
Nachrichten über Datenschutzverletzungen bei großen Unternehmen häufen sich. Und nicht selten führen sie zu finanziellen Verlusten und einem geschädigten Image. DLP dient als erste Verteidigungslinie gegen solche Vorfälle.

Einhaltung gesetzlicher Vorschriften
Gesetze wie die DSGVO, HIPAA und viele andere schreiben strenge Datenschutzstandards vor. DLP-Lösungen stellen sicher, dass Unternehmen diese Vorschriften einhalten, indem sie unbefugte Datenzugriffe und -übertragungen verhindern.

Schutz des geistigen Eigentums
Geistiges Eigentum ist oft das Rückgrat eines Unternehmens und DLP stellt sicher, dass nur befugte Mitarbeitende auf diese wichtigen Daten zugreifen können.

// Security Awareness

Die Mitarbeitenden sind mitunter das schwächste Glied in einer Security-Strategie. Denn ihr Verhalten ist schwer vorauszusagen und wir wissen aus eigener Erfahrung, dass menschliche Fehler zwar selten, aber unvermeidlich sind. Um den sicherheitsrelevanten Auswirkungen eines bewussten oder unbewussten Fehlverhaltens seitens der Endanwender zuvorzukommen, ist es wichtig, sie zu sensibilisieren. Und dafür gibt es ganz unterschiedliche Methoden.

Um die Security Awareness in der Belegschaft zu stärken, hilft es zunächst, den Menschen nicht vorrangig als Sicherheitslücke zu begreifen, sondern vielmehr als zusätzlichen Abwehrschirm gegen Cyberangriffe. Den Mitarbeitenden sollte entsprechend motivierend und praxisnah vor Augen geführt werden, dass ihr Verhalten aktiv dazu beitragen kann, ihren Arbeitgeber und somit auch ihren Job zu schützen. Sie müssen erfahren, dass sie nicht Ursache des Problems sind, sondern ein essenzieller Teil der Sicherheitslösung – eine Erkenntnis, die persönlich dazu anspornt, auf einen sicheren digitalen Umgang zu achten.

Doch auf welche Maßnahmen kann ich setzen, um eine Bewusstseinsschärfung zu erreichen? Die Antwort darauf hängt von dem jeweiligen Zielpublikum ab. Möchte man eine möglichst große Masse erreichen, eignen sich vor allem interne Awareness-Trainings, die zwar inhaltlich übersichtlich, dafür aber für das gesamte Personal verpflichtend sind. Diese können entweder virtuell oder in Präsenz stattfinden und sollten im Idealfall regelmäßig und in festen Zeitintervallen stattfinden. Als Initiator fungieren hierbei oftmals die IT oder – wo vorhanden – die Abteilungen Informationssicherheit und Datenschutz, die dafür sorgen, dass alle wesentlichen Sicherheitsthemen im Rahmen der Schulung zur Sprache kommen.

Ein weiteres Mittel, das zu einer breiten Bewusstseinsbildung beiträgt, ist die Phishing-Simulation. Hierbei versenden Unternehmen meist mit Vorankündigung und mithilfe eines Tools immer wieder gefälschte Phishing-E-Mails oder -Nachrichten an ihre eigenen Mitarbeitenden, um deren Reaktion auf diese betrügerischen Versuche zu testen. Die Vorteile: Die Endanwender werden darauf trainiert, Phishing-Versuche zu erkennen und ihre Fähigkeiten im Umgang mit diesen E-Mails zu verbessern. Gleichzeitig erhält die IT-Abteilung in regelmäßigen Abständen einen Status quo darüber, wie es mit der internen Awareness bestellt ist.

Nun gibt es neben der gesamten Belegschaft in jedem Unternehmen aber auch kleinere Gruppen, die aufgrund ihrer Rolle oder Funktion gesonderte und zugleich umfassendere Schulungen benötigen. Diese sollten im Rahmen von interaktiven Workshops erfolgen, die speziell auf vorhandene Use Cases ausgerichtet sind. Im Kontext der Workspace Security können hierbei vor allem Change oder Transformation Manager unterstützen, die über die entsprechende Methodenkompetenz verfügen und gleichzeitig wissen, auf was es beim Zusammenspiel von Mensch und Technologie ankommt.

Awareness-Kampagnen gehören zu den wichtigsten und sinnvollsten Präventivmaßnahmen. Doch sie sind und bleiben nur ein kleiner Teil im Kontext einer ganzheitlichen Cybersecurity-Strategie. Wichtig ist zuallererst, auf die richtigen Technologien, Lösungen und Werkzeuge zu setzen, die ein sicheres hybrides Arbeiten ermöglichen, um dann im direkten Anschluss die Endanwender zu befähigen, mit diesen Tools versiert und umsichtig umzugehen.

// Security Monitoring & Reporting

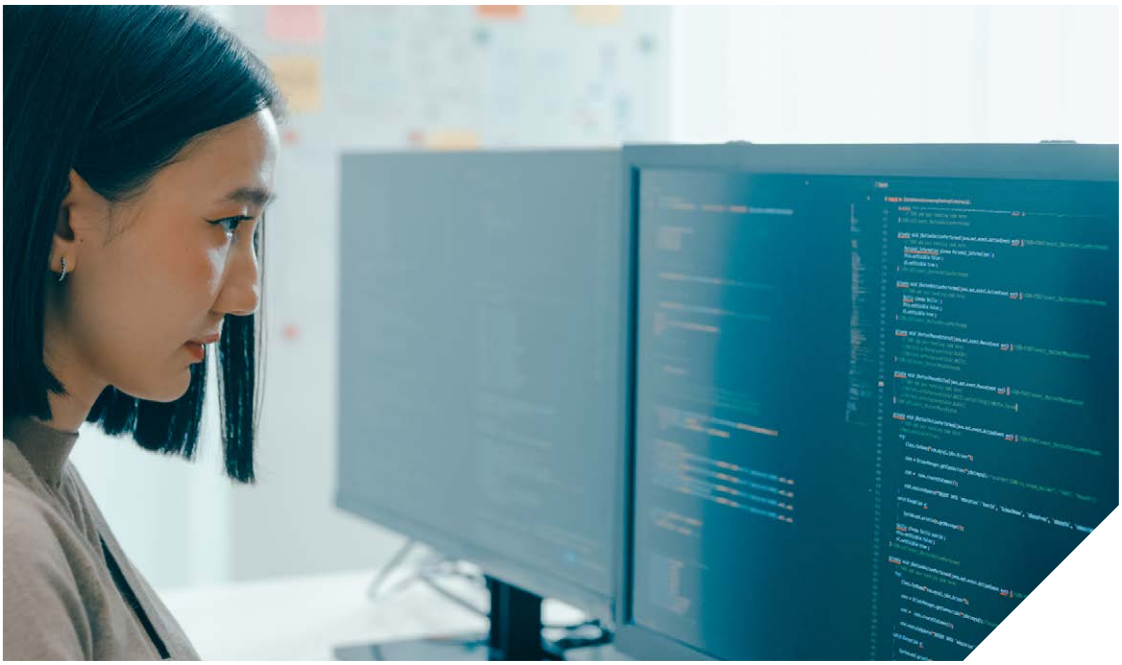
Wissen, was läuft – und das bestenfalls in Echtzeit. Eine kontinuierliche Überwachung und Protokollierung aller Netzwerk- und Dateiaktivitäten gehört zu den wichtigsten Prinzipien einer Zero-Trust-Architektur und wird damit für jedes Unternehmen zur Pflicht, auch unter Compliance-Gesichtspunkten. Denn nur wer vollständige Transparenz schafft, ist in der Lage, potenzielle Sicherheitsbedrohungen sowie ungewöhnliches Benutzerverhalten bereits mit ihrem Auftreten zu erkennen und entsprechende Gegenmaßnahmen einzuleiten.

Damit ein solches Monitoring in seiner Komplexität gewährleistet werden kann, ist der Einsatz intelligenter Technologien unabdingbar. Etabliert haben sich in diesem Zusammenhang UEBA-, SIEM-, EDR-/XDR- und SOAR-Lösungen, auf die im Folgenden näher eingegangen wird.

User and Entity Behavior Analytics (UEBA)
UEBA bezeichnet eine Technologie, die Verhaltensanalysen, Algorithmen für maschinelles Lernen und Automatisierung einsetzt, um abnormales und potenziell gefährliches Benutzer- und Geräteverhalten zu identifizieren. Dies dient vor allem dem Aufdecken von Insider-Bedrohungen, die anderen Tools entgehen können. Obwohl UEBA als eigenständiges Produkt verwendet werden kann, sollte es als ein Werkzeug in der umfassenden Cybersicherheits-Toolbox betrachtet werden. Entsprechend sind heutzutage Lösungen für SIEM, EDR oder IAM mit umfangreichen UEBA-Funktionen ausgestattet.

Security Information and Event Management (SIEM)
SIEM steht für eine Sicherheitslösung, mit der Unternehmen mögliche Sicherheitsbedrohungen und Schwachstellen in ihrer IT-Infrastruktur in Echtzeit erkennen und beheben können. Nicht nur werden durch integrierte UEBA-Funktionen Unregelmäßigkeiten im Benutzerverhalten identifiziert, auch können manuelle Prozesse für das Aufspüren von Bedrohungen sowie die Reaktion auf Vorfälle mithilfe von Künstlicher Intelligenz automatisiert werden. Zudem eignen sich SIEM-Lösungen sehr gut für die Durchführung computerforensischer Untersuchungen und ermöglichen weiterhin eine ganzheitliche Überwachung der Einhaltung gesetzlicher Vorschriften.

Security Orchestration, Automation and Response (SOAR)
SOAR-Plattformen kommen vor allem in solchen Unternehmen zum Einsatz, in denen ein ganzes Team von IT-Sicherheitsexperten damit beschäftigt ist, die komplette IT-Infrastruktur rund um die Uhr zu überwachen. Diese Teams, auch bekannt als Security Operations Center (SOC), nutzen hierfür bis zu 100 unterschiedliche Sicherheitslösungen, die sich darum kümmern, Cyberattacken aufzuspüren und abzuwehren. Die Schwierigkeit dabei: Diese Tools sind nicht immer so konzipiert, dass sie optimal zusammenzuarbeiten, was schlimmstenfalls dazu führt, dass SOCs bei jeder einzelnen Reaktion auf einen Sicherheitsvorfall die benötigten Tools manuell integrieren müssen. SOAR-Lösungen schaffen hier Abhilfe, denn sie bieten Sicherheitsteams eine zentrale Konsole, über die sich die separaten Tools in optimierte Workflows zur Reaktion auf Bedrohungen integrieren und koordinieren lassen. Auch können einfache, sich wiederholende Aufgaben in diesen Workflows automatisiert werden, was die Arbeit des SOCs deutlich erleichtert.



Extended Detection and Response (XDR)
XDR ist die Weiterentwicklung von EDR. Anders als EDR, das Aktivitäten über mehrere Endpunkte hinweg sammelt und korreliert, erweitert XDR den Erkennungsbereich über die Endpunkte hinaus und bietet Erkennung, Analyse und Reaktion über Endpunkte, Netzwerke, Server, Cloud-Workloads, SIEM und vieles mehr. Wie SOAR-Integrationen können auch XDR-Lösungen automatisch auf Sicherheitsereignisse reagieren. Dabei ermöglichen sie jedoch weitaus komplexere und umfassendere Automatisierungen, als es SOAR zulässt. Weitere Vorteile gegenüber SOAR sind die vereinfachte Integration von Sicherheitstools sowie die Tatsache, dass die Nutzung von XDR weniger Fachwissen erfordert und geringere Kosten verursacht.

SIEM, SOAR, XDR – während SecOps-Teams in großen Unternehmen häufig all diese Tools gleichzeitig verwenden, sehen kleine und mittlere Unternehmen angesichts des Fachkräftemangels oftmals keine Möglichkeit, ein solches Security Monitoring im Alleingang zu bewältigen. Doch das müssen sie auch gar nicht, denn mittlerweile lassen sich Security-Leistungen ganz einfach als Service konsumieren! Dies ist oftmals nicht nur kostengünstiger als eine Überwachung in Eigenregie, sondern auch ressourcenschonender, da die Verantwortung nun bei externen Experten liegt.

Eine gute Vorbereitung ist das A und O

Eine Zero-Trust-Architektur lässt sich nicht auf die Schnelle aufbauen – auch dann nicht, wenn mit der Workspace Security nur ein Teilbereich der unternehmensweiten IT-Sicherheitsstrategie betrachtet wird. Stattdessen ist zunächst eine gewisse und oftmals zeitintensive Vorarbeit notwendig. Denn bevor die ersten konkreten Maßnahmen geplant, implementiert und umgesetzt werden können, müssen zuerst einmal die Ressourcen identifiziert werden, die es zu schützen gilt. Und das erfordert nicht selten die Mitarbeit weiterer Organisationseinheiten, insbesondere dann, wenn es darum geht, die schützenswerten Ressourcen aus den Geschäftsprozessen zu bestimmen.

Folgende Aspekte sind somit Voraussetzung, damit die neu zu errichtende Zero-Trust-Architektur von Beginn an auf stabilen Beinen steht:[16]

1. Identifizieren und Priorisieren der zentralen Geschäftsprozesse einer Organisation

Für Zero-Trust-Architekturen wird dabei eine deutlich differenziertere Ausarbeitung der Geschäftsprozesse nötig, als sie derzeit in vielen Organisationen vorliegt. Wichtig ist in diesem Zusammenhang vor allem die Abbildung der Kernprozesse, die über die unterstützenden Prozesse beispielsweise der IT hinausgehen.

2. Identifizieren aller beteiligten Parteien innerhalb der Organisation

Hierbei muss herausgearbeitet werden, welche Organisationseinheiten in den jeweiligen Geschäftsprozessen involviert sind. Hieraus ergeben sich dann die Rollen, die im weiteren Verlauf u. a. als Grundlage für Zugriffsentscheidungen dienen.

3. Identifizieren von regulatorischen Vorgaben

Bei der Umsetzung sind Vorgaben zu berücksichtigen, die sich aus Gesetzen, Verordnungen oder anderen Rechtseinflüssen ergeben können und gegebenenfalls Einfluss auf die umzusetzenden Maßnahmen bzw. deren Reihenfolge haben.

4. Identifizieren aller involvierten Ressourcen der Organisation

Aus den erarbeiteten Geschäftsprozessen müssen die involvierten Ressourcen, darunter vor allem Daten, Systeme und Anwendungen, abgeleitet werden. Denn nur so lassen sich in einer Zero-Trust-Architektur feingranulare Zugriffsregeln definieren.

5. Formulierung von Sicherheitsrichtlinien, die Zero-Trust-Maßnahmen beinhalten

Diese Formulierungen dienen als Fundament für spätere Zugriffsentscheidungen, welche Entitäten auf die Ressourcen zugreifen dürfen und unter welchen Bedingungen das geschehen muss. Daraus lassen sich wiederum maschinenlesbare Attribute ableiten.

6. Markterkundung

Für einen ganzheitlichen Einsatz von Zero Trust ist eine umfangreiche Recherche nach geeigneten Produkten unerlässlich. Denn die eine Zero-Trust-Lösung gibt es nicht; es braucht stattdessen viele einzelne Sicherheitstools, die in ihrem Zusammenwirken eine effiziente Architektur gegen Angreifer schaffen. Entsprechend ist bei der Recherche auch zu prüfen, inwieweit die verschiedenen Produkte miteinander harmonieren.

7. Priorisierung der Umsetzung

Dabei sind u. a. Aspekte wie die Abhängigkeit von Clientkomponenten bzw. deren Sicherheitszustand, das Vorhandensein von adäquaten Loginformationen und (offenen) Protokollschnittstellen sowie notwendige Prozessänderungen zu berücksichtigen.

[16] *Bundesamt für Sicherheit in der Informationstechnik, Positionspapier Zero Trust 2023*

5/ Der Blick in die Zukunft.
Spannend und wertvoll.

Trend No. 1: KI-gestützte Cybersecurity

Künstliche Intelligenz ist das Thema der heutigen Zeit. Und während Cyberkriminelle die KI schon längst für sich entdeckt haben, setzen Softwarehersteller derzeit alles daran, Lösungen zu schaffen, die in der Lage sind, KI-basierten Angriffen mit einer KI-gestützten Abwehr zielgerichtet entgegenzutreten. Die Möglichkeiten hierfür sind vielfältig und erstrecken sich von der Identifikation von Phishing-Mails über den Schutz vor Trojanern und Malware bis hin zur Authentifikation und Identifikation von Nutzern oder die Entwicklung sicherer Software. Grundsätzlich liegt aber der größte Vorteil darin, dass die KI die Basis für Echtzeit-Überwachung und detaillierte Analyseverfahren bietet und vor allem eine Entlastung der IT-Sicherheitsteams bedeutet.

Trend No. 2: Cloud Security

Angesichts der fortschreitenden Migration von Unternehmen in die Cloud steigt die Notwendigkeit einer umfassenden Strategie zur Cloudsicherheit rapide an. Die meisten Cloud-Anbieter befolgen zwar standardmäßig bewährte Sicherheitsverfahren und ergreifen aktiv Maßnahmen zum Schutz der Integrität ihrer Server. Dennoch müssen Unternehmen unbedingt eigene Vorkehrungen zur Absicherung ihrer Daten, Anwendungen und Workloads treffen, die in der Cloud ausgeführt werden. Hilfestellung bei der Suche eines dafür geeigneten Ansatzes liefert das National Institute of Standards (NIST). Das NIST hat eine Liste von Best Practices für die Einrichtung eines sicheren und nachhaltigen Cloud-Computing-Rahmens erstellt, die jedes Unternehmen in die Lage versetzen, die Sicherheitsbereitschaft selbst zu bewerten und angemessene präventive und restaurative Sicherheitsmaßnahmen zu ergreifen. Zudem existiert mit Cloud Security Posture Management (CSPM) eine neue Technologie, die die Umsetzung des NIST-Rahmens für Cybersicherheit unterstützt, indem sie Fehlkonfigurationen in Cloud-Umgebungen erkennt und behebt.

Trend No. 3: SOC as a Service

Managed Services und „as-a-Service"-Modelle sind im Trend. Und insbesondere im Bereich Cybersicherheit wächst der Bedarf an IT-Security-Dienstleistungen im Allgemeinen und SOC-Services im Speziellen. Die Gründe hierfür sind einleuchtend: Die Komplexität der IT-Infrastruktur nimmt stetig zu; gleichzeitig braucht es heutzutage sehr gut ausgebildete Security-Spezialisten, die diese Komplexität in ihrer Tiefe begreifen müssen, um geeignete Schutzmaßnahmen zu entwickeln und umzusetzen. Doch immer mehr Unternehmen können auf solche Expertise aus den eigenen Reihen nicht zählen, weshalb sich die hybride Zusammenarbeit zwischen internen Teams und externen Dienstleistern zunehmend von einem einstigen Zukunftsmodell zu einem etablierten Gegenwartsmodell entwickelt.

Trend No. 4: Blockchain

Die Blockchain-Technologie wird in der Cybersecurity zunehmend an Bedeutung gewinnen. Denn die dezentralisierte Ledger-Technologie ist für ihre inhärenten Sicherheitsmerkmale wie Unveränderlichkeit, Transparenz und Manipulationssicherheit bekannt, wodurch sie Datenmanipulation erheblich erschwert. Befinden sich Daten in einer Blockchain, können sie ohne den Konsens des Netzwerks nicht verändert werden, was gerade beim Schutz sensibler Daten ein entscheidender Vorteil ist. Außerdem können Organisationen in der Blockchain besser kontrollieren, wer auf Daten zugreift und so das Risiko von Identitätsdiebstahl und Betrug verringern.

Trend No. 5: OT Security – Industrial Internet of Things

Die zunehmende Digitalisierung und Vernetzung in der Industrie 4.0 führt zu neuen Herausforderungen im Bereich der Betriebstechnologie (OT). Cyberangriffe werden spezialisierter und gefährden nicht nur IT-Systeme, sondern zunehmend auch OT-Komponenten. Und das betrifft Unternehmen des produzierenden Gewerbes genauso wie die Energiewirtschaft, das Gesundheits- und Krankenhausumfeld sowie alle Branchen mit kritischer Infrastruktur. Entsprechend erfordern OT-Umgebungen maßgeschneiderte Sicherheitsmaßnahmen, die auf die Besonderheiten der industriellen Steuerung und der physischen Prozesskontrolle zugeschnitten sind. Es ist wichtig, Sicherheitsstrategien zu implementieren, die die Schutzziele und die Funktionalität von OT-Systemen gleichermaßen berücksichtigen.

Trend No. 6: Post-Quanten-Kryptografie

Es gibt kaum noch Zweifel daran, dass die Quanten-Technologie irgendwann im Mainstream ankommen und in der Breite verfügbar sein wird. Und sobald das geschieht, könnte die überlegene Rechenleistung der Quantencomputer Verschlüsselungen brechen, die heute als sicher gelten. Um zu verhindern, dass Cyberkriminelle diese neuen Möglichkeiten für sich nutzen, werden bereits neue Verschlüsselungsalgorithmen entwickelt, die derartig komplex sind, dass sie auch mit Quantenrechnern nicht in reeller Zeit geknackt werden können. Unternehmen, die sich zukunftssicher aufstellen wollen, sollten also schon heute auf Kryptoagilität setzen, was bedeutet, die kryptografischen Systeme so auszulegen, dass sich Soft- und Hardware auf die neuen quantensicheren Algorithmen umstellen lassen, sobald diese notwendig werden.

6/ Resümee.
Bleiben Sie sicher unterwegs!

Keine Macht den Cyberkriminellen! – Zugegeben: Dieser Aufruf scheint angesichts der aktuell akuten Bedrohungslage eher unrealistisch als machbar, doch der Schein trügt. Denn Fakt ist, dass Angreifer nur mit so viel Macht aufwarten können, wie Sie es zulassen. Es sind schließlich Sie, der als Gewinner hervorgeht, wenn eine Attacke dank Ihrer Sicherheitsmaßnahmen erfolglos bleibt. Und somit sind es auch Sie, der dem Angreifer damit jegliche Macht aberkennt. Sich dieser Tatsache bewusst zu sein und sie sich auch immer wieder vor Augen zu führen, hilft, sich mit Ruhe und Gelassenheit den alltäglichen Security-Herausforderungen zu stellen und eine Strategie zu entwerfen, mit der Sie die Oberhand gewinnen und behalten.

Einfach ist das sicherlich nicht, denn um einen passenden Schutzschild für die Unternehmens-IT zu konzipieren, braucht es die richtige Expertise und vor allem ein gemeinsames Verständnis darüber, was Zero Trust für das eigene Unternehmen bedeutet. Dieses Verständnis bildet die Grundlage für die Strategieentwicklung und sollte so dokumentiert werden, dass es im weiteren Verlauf auch für neue Stakeholder leicht nachvollziehbar ist.

Nun birgt insbesondere die hybride Arbeitsweise verbunden mit dem digitalen Arbeitsplatz neue, teils noch unbekannte Security-Herausforderungen, die es möglichst schnell anzugehen gilt. Das Gute daran ist, dass es für jede von ihnen bereits großartige Ansätze und Lösungen gibt! Die Kunst besteht eher darin, die für sich geeigneten Sicherheitslösungen zu identifizieren und gleichzeitig sicherzustellen, dass diese miteinander harmonieren. Ist das geschafft und sind zusätzlich alle Mitarbeitenden sensibilisiert, können Sie sicher sein, fortan einen funktionierenden und rundum abgesicherten Digital Workspace Ihr Eigen nennen zu dürfen.

Damit Sie sich nun frohen Mutes ans Werk machen können, möchten wir Ihnen noch einen letzten, wertvollen Rat mit auf den Weg geben: „Gut Ding will Weile haben“. Genauso wie Rom kann auch eine Zero-Trust-Architektur nicht an einem Tag erbaut werden. Entsprechend sollten Sie sich Zeit nehmen und diese zuallererst in die Formulierung einer ganzheitlichen IT-Sicherheitsstrategie investieren, die sowohl alle relevanten Aspekte Ihrer Infrastruktur miteinbezieht als auch fortschrittlich und aussagekräftig ist. Steht diese Grundlage, so wird es im Anschluss vergleichsweise einfach sein, daraus die wichtigsten Handlungsfelder abzuleiten und anzugehen. Und dabei gilt:

Jeder noch so kleine Schritt bringt einen vorwärts.

Los geht’s!

7/ SVA.
Ihr kompetenter Ansprechpartner.

Der moderne Arbeitsplatz lebt von den Möglichkeiten, die er schafft. Er bringt Menschen aus verschiedenen Orten virtuell zusammen, lässt sie miteinander kommunizieren, kollaborieren und produktiv sein. Doch das ist alles nichts wert, wenn die Sicherheit darunter leidet und damit die Existenz des Unternehmens potenziell gefährdet ist. **Deshalb kommen wir ins Spiel!**

Als einer der führenden IT-Dienstleister in Deutschland begleitet SVA Organisationen seit Jahren professionell beim Aufbau digitaler Arbeitsplatzumgebungen und dem damit verbundenen Transformationsprozess innerhalb der Belegschaft. Hierbei helfen uns die richtigen Kompetenzschwerpunkte – gegliedert in eng verzahnte Fokusbereiche, die stets in regem Austausch stehen, um im Zusammenspiel die bestmögliche Lösung für unsere Kunden zu erarbeiten. Diese Haltung, gepaart mit dem Projekt-Know-how unserer Experten, dem hochwertigen Produktportfolio und dem Blick fürs Ganze machen SVA zum idealen Begleiter auf dem Weg zu einem digitalen Arbeitsplatz, der jegliche Anforderungen in Sachen Sicherheit, Verfügbarkeit und Performance erfüllt.

- **Großes Expertenteam im Bereich End-User Computing und Cybersecurity**
- **Bestes Know-how in Sachen Digital Workspace, Zero Trust, Cloud, Network und KI**
- **Langjährige Partnerschaften mit den wichtigsten Lösungsanbietern**
- **Gelebte Zusammenarbeit auf Augenhöhe, geprägt von Sachverstand, Ergebnisorientierung und Neutralität**
- **Tiefes Verständnis für kundenspezifische Business- und Nutzeranforderungen**

BeyondTrust · CHECK POINT · Cisco Partner Gold Integrator · citrix Partner Platinum Plus · CYBERARK The Identity Security Company · Delinea · deviceTRUST Certified Partner · exabeam · FORTINET · IBM Platinum Partner · imprivata Authorized Partner · ivanti · jamf · MATRIX42 Competence Partner 2024 Platinum · Microsoft Solutions Partner Security · mondoo

Verweise

Bundesamt für Sicherheit in der Informationstechnik (BSI), Lagebericht „Die Lage der IT-Sicherheit in Deutschland 2023“ vom 02.11.2023. In: bsi.bund.de. Unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html [Stand: 04.07.2024]

TÜV-Verband, Studie „Cybersecurity Studie 2023“ vom 12.06.2023. In: tuev-verband.de. Unter: https://www.tuev-verband.de/studien?tx_news_pi1%5Bnews%5D=671 [Stand: 04.07.2024]

Surfshark, Online-Artikel „Cybercrime statistics“ von 2023. In: surfshark.com. Unter: https://surfshark.com/research/data-breach-impact/statistics [Stand: 04.07.2024]

Bitkom e.V., Studie „Wirtschaftsschutz 2023“ von 2023. In: bitkom.org. Unter: https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz [Stand: 04.07.2024]

WEKA Fachmedien, Studie „Digital Workplace 2021/2022“ von 2022, In: info.logitech.com. Unter: https://info.logitech.com/2122-digital-workplace-study-de-de.html [Stand: 08.02.2024]

Heise Online, Artikel „Continental: IT-Einbruch erfolgte über heruntergeladenen Browser von Mitarbeiter“ vom 14.12.2022. In: heise.de. Unter: https://www.heise.de/news/Continental-IT-Einbruch-erfolgte-ueber-heruntergeladenen-Browser-von-Mitarbeiter-7394151.html [12.03.2024]

Bayerischer Rundfunk (BR), Artikel „Phishing-Vorfall beim BR“ vom 17.02.2023, In: br.de. Unter: https://www.br.de/unternehmen/pishing-angriff-br-100.html [Stand: 12.03.2024]

Heinrich Heine Universität Düsseldorf (HHU), Artikel „Daten aus E-Mails der HHU entwendet“ vom 14.07.2023, In: hhu.de. Unter: https://www.hhu.de/news-einzelansicht/daten-aus-e-mails-der-hhu-entwendet [Stand: 12.03.2024]

Bundesamt für Sicherheit in der Informationstechnik (BSI), Publikation „Positionspapier Zero Trust 2023“ vom 04.07.2023. In: bsi.bund.de. Unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.html [Stand: 04.07.2024]

Kontakt

Stefan Müller
Head of Business Line End-User Computing

SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
Tel.: +49 151 18 025 702
E-Mail: stefan.mueller@sva.de

SVA gehört zu den führenden IT-Dienstleistern Deutschlands und beschäftigt mehr als 3.000 Mitarbeiter an 27 Standorten. Das unternehmerische Ziel von SVA ist es, hochwertige IT-Produkte der jeweiligen Hersteller mit dem Projekt-Know-how, dem Service-Spektrum und der Flexibilität von SVA zu verknüpfen, um so optimale Lösungen für die Kunden zu erzielen.

Fokusbereiche der SVA:
> Agile IT & Software Development
> Big Data Analytics & IoT
> Business Continuity
> Cybersecurity
> Datacenter Infrastructure
> Digital Process Solutions
> End-User Computing
> Mainframe
> SAP

Gestaltung: Lindenmayer+Lehning, Darmstadt