2024

IT Security First: Mit fünf Maßnahmen schnell zu 99 Prozent Sicherheit

FEHLENDE IT-SECURITY: DIE UNBEACHTETE EXISTENZBEDROHUNG FÜR DEN MITTELSTAND

CHRISTOPH ZAPATKA | PRINCIPAL PRESALES CONSULTANT

Inhaltsverzeichnis

Management Summary 2

So einfach können sich Unternehmen vor einer Attacke schützen 3

Gut zu wissen: Wie laufen Attacken ab? 4

- Mitre Att&ck Framework 4
  - Eine Übersicht über die zentralen Taktiken zeigt das Mitre-Att&ck Schema 5
- Maßnahme 1: Multi-Faktor-Authentifizierung 7
- Maßnahme 2: Zero Trust Strategie 8
  - Authentifizierung und Autorisierung 10
  - Verringern der Angriffsfläche 12
- Maßnahme 3: Extended Detection and Response 17
- Maßnahme 4: Up to date bleiben 20
- Maßnahme 5: Daten schützen 21

Informationen zur Bedrohungslage – wie arbeiten Cyber-Kriminelle? 22

- Was ist Ransomware-as-a-Service? 23
- Überblick häufig verwendeter Ransomware bei deutschen Zielen 24
  - Eine unvollständige Übersicht erfolgreicher Angriffe im vierten Quartal 2023 26
  - Einschätzung der Bedrohungslage deutscher Unternehmen 27
- Wie bekommen die Angreifer Zugriff auf die Systeme 27
  - Phishing wächst kontinuierlich. 27
  - Die Zahl der Angriffe auf Identitäten ist drastisch gestiegen. 30
- Warum werden Identitäten gestohlen? 30

Management Summary

Die Menge der Angriffe auf IT-Infrastruktur nimmt konsequent zu. Mit einer durchschnittlichen Schadenssumme von 4 Millionen Euro und einer Schadenssumme im Jahr 2023 von 203 Mrd. Euro gehört Cybercrime weiter zu den Bereichen mit dem höchsten Schadenspotenzial in Deutschland. Obwohl die Angriffsfläche laut dem Microsoft Digital Defense Report mit 5 einfachen Schritten um 99% verringert werden kann, sprechen die Zahlen, die das BKA und die Bitkom vorlegen, eine beängstigende Sprache.

Der Großteil der befragten Unternehmen setzt leider die Best Practices nicht um und wiegt sich im trügerischen Glauben, kein attraktives Ziel zu sein. Ein Beispiel dafür ist die beängstigend niedrige Zahl der geschützten Administratorkonten, die damit Einfallstore für jede Art Angriff sind. Der erfolgreiche Angriff auf die kommunale IT in Nordrhein-Westfalen im Herbst 2023 ist ein Beweis dafür. Jegliche IT-Umgebung ist das Ziel von Cybercrime – es ist nur eine Frage der Zeit, bis die Unternehmen es bemerken. 63 Prozent der befragten Unternehmen gehen von einem Angriff in der nächsten Zeit aus – weniger als die Hälfte sieht sich dafür gut genug gerüstet. Grund dafür könnte unter anderem sein, dass der Großteil der Deutschen immer noch auf schwache Passwörter wie „123456789!“ setzt, wie das Hasso-Plattner-Institut berichtet. Die Kombination aus Username & Passwort ist hochgradig unsicher und wird doch ohne weitere Schutzebene in sehr vielen Unternehmen verwendet.

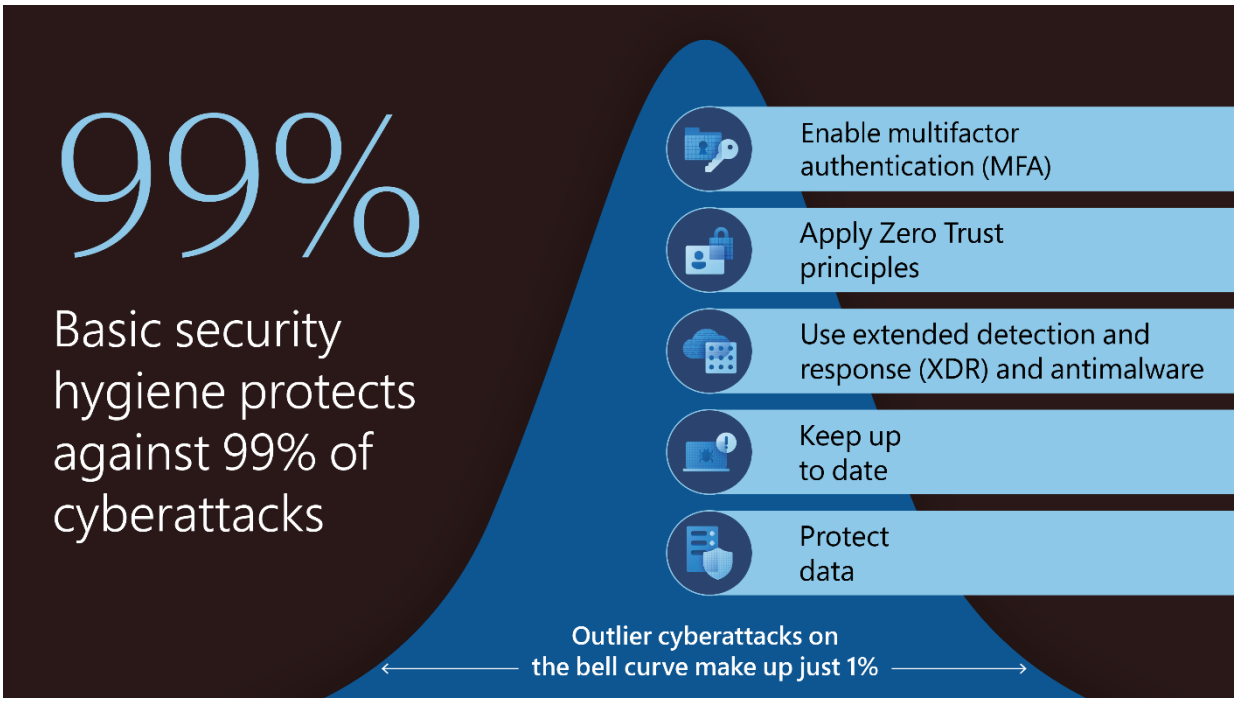
Höchste Zeit, das zu ändern und Angreifer zu stoppen.

In diesem Whitepaper stellen wir effektive Schutzmaßnahmen vor, mit denen Sie sich mit geringem Aufwand vor Angriffen schützen und die Folgen bereits erfolgter Angriffe reduzieren können.

So einfach können sich Unternehmen vor einer Attacke schützen

Wenn der Großteil der Unternehmen mit einer Cyberattacke rechnet, dann stellt sich die Frage, wie sie sich davor schützen wollen. Basierend auf der Umfrage der Bitkom kann über die Hälfte der Unternehmen diese Frage nicht beantworten. Es ist leicht, diesen Unternehmen Fahrlässigkeit, Ignoranz oder Geiz vorzuwerfen. Es ist jedoch komplett falsch.

Unternehmen, die jetzt anfangen ihre Sicherheitskonzepte zu überarbeiten (oder zu erstellen), sehen sich einem Dschungel von Maßnahmen gegenübergestellt, die eigentlich alle gleichzeitig umgesetzt werden sollten.



Indem Sie diese fünf einfachen Schritte schnellstmöglich umsetzen, können Unternehmen ihre Umgebung erfolgreich absichern:

1. Multifaktor-Authentifizierung durchsetzen
2. Zero-Trust Prinzipien einführen
3. Erweiterte Erfassungs- und Reaktionssysteme (XDR) einsetzen
4. Up to date bleiben (Updates, Upgrades)
5. Daten schützen

Gut zu wissen: Wie laufen Attacken ab?

Bei den meisten Angriffen stellen wir fest, dass die Angreifer über längere Zeit in der Umgebung „heimisch“ geworden sind, um den für sie sichersten Punkt zu finden, diesen Angriff zu starten.

Besonders in größeren Umgebungen planen Angreifer eine längere Phase der Erkundung ein, um so den größtmöglichen Impact zu erzielen. Vergessen wir nicht, dass Angreifer diese Schritte geschäftsmäßig betreiben und daher versuchen, ihre Kosten-Nutzen-Rechnung so erfolgreich wie möglich zu betreiben. Es ist daher nicht ungewöhnlich, dass ein System schon einige Monate in der Hand der Hacker ist, bevor diese sich bemerkbar machen.

In dieser Zeit wird versucht, den Angriff so breit wie möglich aufzustellen, indem Schadcode in der gesamten Infrastruktur ausgebreitet wird. Die Angreifer schaffen sich so „Back-Ups“, für den Fall, dass ihr Vorgehen an einer Stelle eventuell bemerkt werden sollte.

Es ist entscheidend für die Sicherheit einer IT-Umgebung, die einzelnen Schritte und Phasen eines Angriffs, bzw. einer Infiltration ihres Unternehmens zu verstehen.

Mitre Att&ck Framework

MITRE ATT&CK® ist eine weltweit zugängliche Wissensbasis über Taktiken und Techniken von Angreifern, die auf realen Beobachtungen beruht. Die ATT&CK-Wissensbasis wird als Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und -methoden im privaten Sektor, in der Regierung und in der Gemeinschaft der Cybersicherheitsprodukte und -dienstleistungen verwendet. ATT&CK ist offen und steht jeder Person oder Organisation zur kostenlosen Nutzung zur Verfügung. (https://attack.mitre.org/)

Das ATT&CK Framework beschreibt 14 Angriffskategorien, die in mehrere Subkategorien unterteilt werden. Diese können wiederum weitere Unterordnungen beinhalten.

Die dadurch entstehende Matrix ist dementsprechend vielfältig und wird hier nur am Beispiel der ersten Kategorie „Aufklärung“ (Reconnaissance) beschrieben:

> *Bei der Aufklärung handelt es sich um Techniken, bei denen der Gegner aktiv oder passiv Informationen sammelt, die zur Unterstützung von Angriffen verwendet werden können. Zu diesen Informationen können Einzelheiten über die Organisation des Opfers, die Infrastruktur oder das Personal gehören. Diese Informationen können vom Angreifer genutzt werden, um andere Phasen des Lebenszyklus des Angreifers zu unterstützen, z. B., um den Erstangriff zu planen und auszuführen, um Ziele nach der Kompromittierung festzulegen und zu priorisieren oder um weitere Aufklärungsbemühungen voranzutreiben und zu leiten.*

Die Taktik „Aufklärung“ dient in erster Linie dazu, herauszufinden, wie sicher eine Umgebung ist, wo sich Schwachstellen mit geringem Aufwand ausnutzen lassen und wo der geringste Widerstand zu erwarten ist.

Dazu zählen:

- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains

Eine Übersicht über die zentralen Taktiken zeigt das Mitre-Att&ck Schema

Erklärung der verschiedenen Taktiken:

1. **Aufklärung**: Sammeln von Informationen zur Planung künftiger gegnerischer Operationen, d.h. Informationen über die Zielorganisation
2. **Ressourcenentwicklung**: Aufbau von Ressourcen zur Unterstützung von Operationen, also Einrichtung einer Befehls- und Kontrollinfrastruktur
3. **Erstzugang**: Versuch, in Ihr Netzwerk einzudringen, z. B. Spear Phishing
4. **Ausführung**: Versuch, bösartigen Code auszuführen, z. B. durch Ausführen eines Fernzugriffstools
5. **Hartnäckigkeit**: Versuch, sich weiter zu etablieren, z. B. durch Änderung der Konfigurationen
6. **Privilegienausweitung**: Versuch, höhere Berechtigungen zu erlangen, also Ausnutzung einer Sicherheitslücke, um den Zugriff zu erweitern
7. **Abwehrumgehung**: Versuch, nicht entdeckt zu werden, also dieVerwendung vertrauenswürdiger Prozesse zum Verstecken von Malware
8. **Zugriff auf Anmeldeinformationen**: Stehlen von Kontonamen und Kennwörtern, z. B. Keylogging
9. **Entdeckung**: Versuch, Ihre Umgebung zu erkunden, d. h. herauszufinden, was sie kontrollieren können
10. **Seitliche Bewegung**: Bewegung durch Ihre Umgebung, d. h. Verwendung legitimer Anmeldedaten, um sich durch mehrere Systeme zu bewegen
11. **Sammeln**: Sammeln von Daten, die für das Ziel des Angreifers von Interesse sind, z. B. Zugriff auf Daten im Cloud-Speicher
12. **Command and Control**: Kommunikation mit kompromittierten Systemen, um sie zu kontrollieren, d. h. Nachahmung von normalem Webverkehr, um mit einem Opfernetzwerk zu kommunizieren
13. **Exfiltration**: Diebstahl von Daten, d. h. Übertragung von Daten auf ein Cloud-Konto
14. **Impact**: Manipulation, Unterbrechung oder Zerstörung von Systemen und Daten, z. B. Verschlüsselung von Daten mit Ransomware

Die Komplexität der Angriffsmöglichkeiten zeigt auf, dass ein Service pro Szenario zu einer kompletten Unübersichtlichkeit führen würde, wobei im Umkehrschluss nur die wenigsten Dienste in der Lage sind, diese Komplexität ganzheitlich zu erfassen.

So nachvollziehbar der Wunsch nach einer reinen Tool-Lösung ist, die einmal angeschaltet alle Schwachstellen verschwinden lässt, so wenig realistisch ist dieser Wunsch. Denn neben den bekannten Schwachstellen, wie öffentliche IP-Adressen, zugänglichen Management-Ports oder schwacher Authentifizierung ist die Hauptangriffsstelle immer der Mensch.

Daher nützt das Aktivieren verschiedener Security-Tools vor allem dem Hersteller dieser Tools. Um heutzutage Angriffe effizient abzuwehren und zu verstehen, wo die Schwachstellen sind,

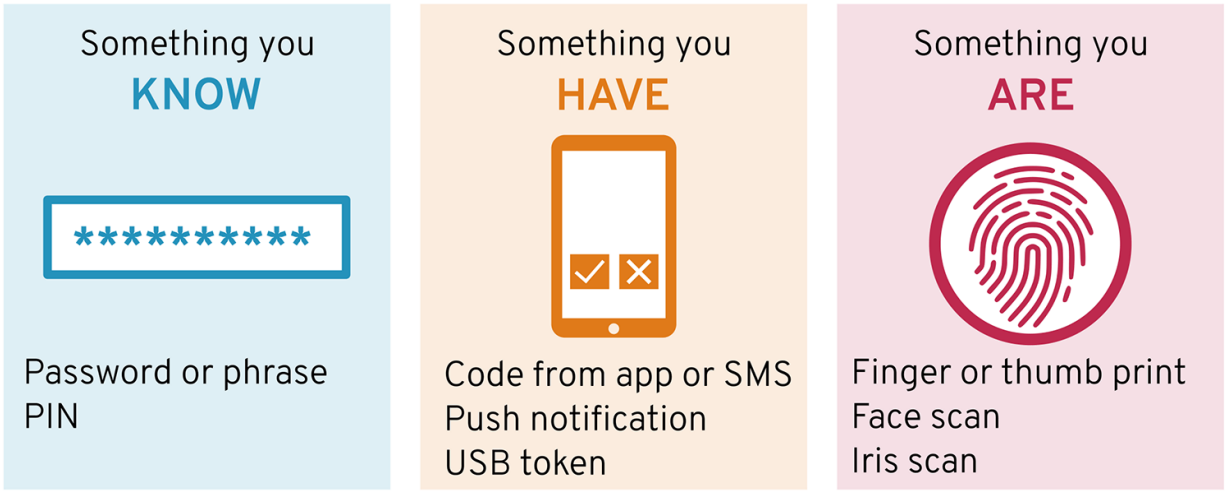
muss eine Security-Strategie erstellt werden, die vor allem den Schutz der Identitäten im Blickwinkel hat.

Maßnahme 1: Multi-Faktor-Authentifizierung

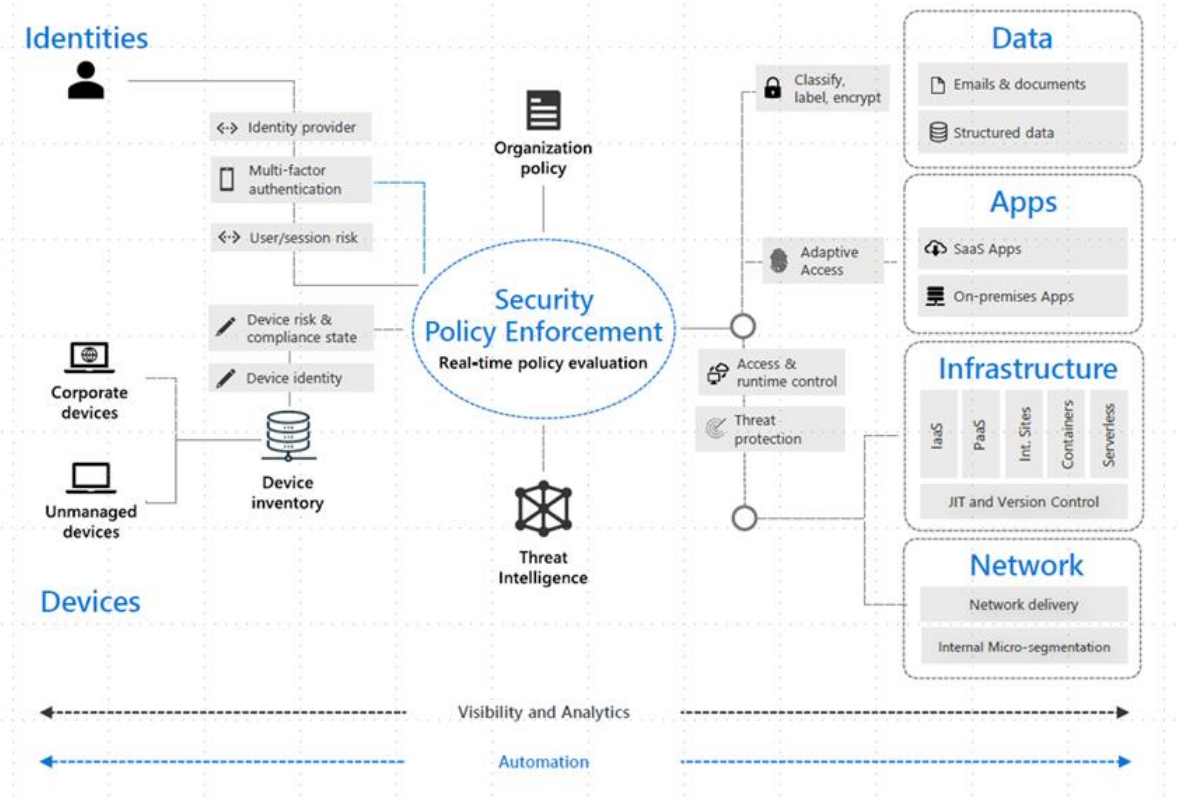
Die Multifaktor-Authentifizierung nutzt im Gegensatz zur Zwei-Faktor-Authentifizierung verschiedene (Multi) Faktoren, um eine Identität zu verifizieren. Die Verifizierung über einen zweiten Faktor nutzt nur einen weiteren Faktor, wie zum Beispiel OTPs (One-Time-Passwords), die mittlerweile als unsicher eingestuft werden, da sie abgefangen und dadurch gefährlich werden können.

MFA ist ein grundlegender Baustein einer Zero Trust Umgebung und folgt dem Grundsatz „Always verify“. Ein zweiter Faktor wird deshalb als entscheidend angesehen, weil nur dadurch sichergestellt werden kann, dass die angegebene Identität verifiziert werden kann. MFA baut auf drei Bausteinen auf:

Etwas, das ich weiß; etwas, das ich kenne; Etwas, das ich bin.



Die Kombination aus diesen drei Bausteinen sichert den Zugriff auf meine (und jede andere) Identität und schützt vor unbefugten Zugriffen. Gemeinsam mit Conditional Access wird eine wesentliche Barriere geschaffen, um Angreifer abzuwehren.



Mit Entra ID P2 als Grundlage einer sicheren Authentifizierung und Autorisierung, der Verbindung aus Conditional Access und einer modernen Multi-Faktor- Authentifizierung kann ein Zero Trust Modell verlässlich und für alle User akzeptabel durchgesetzt werden. Ergänzt werden sollte dieses Konstrukt durch ein XDR-System, das bei der Erkennung und Abwehr von Bedrohungen unterstützt.

Multi-Faktor-Authentifizierung sollte so selbstverständlich sein, wie ein Sicherheitsgurt beim Autofahren: Unvorstellbar, ohne loszufahren.

Maßnahme 2: Zero Trust Strategie

Zero Trust Security ist ein Sicherheitskonzept, das davon ausgeht, dass kein Benutzer, Gerät oder Netzwerk von Natur aus vertrauenswürdig ist. Im Gegensatz zu traditionellen Sicherheitsansätzen, die darauf abzielen, das Innere des Netzwerks als vertrauenswürdig zu behandeln und den Zugriff von innen nach außen zu kontrollieren, legt Zero Trust Security den Schwerpunkt auf eine kontinuierliche Überprüfung und Authentifizierung aller Benutzer und Geräte, unabhängig von ihrem Standort oder ihrer Herkunft.

Zero Trust kann in diesen drei Leitsätzen zusammengefasst werden:

1. Never trust.
2. Always verify.
3. Assume breach.

Die erfolgreiche Umsetzung dieser Sicherheitsarchitektur hängt maßgeblich von der konsequenten Durchsetzung der Zero Trust Grundsätze ab. Das wiederum kann nur gelingen, wenn bei der Umsetzung vor allem auf die Usability, die Anwenderfreundlichkeit geachtet wird. Zero Trust ohne verständliche Usability sorgt für Unzufriedenheit bei den Nutzern und fördert das Entstehen unkontrollierbarer Schatten-IT, in der User sich Schlupflöcher suchen, um den Einschränkungen entgegenzuarbeiten.

Die oben zitierten Leitsätze werden in der Praxis durch diese 5 Einheiten beschrieben:

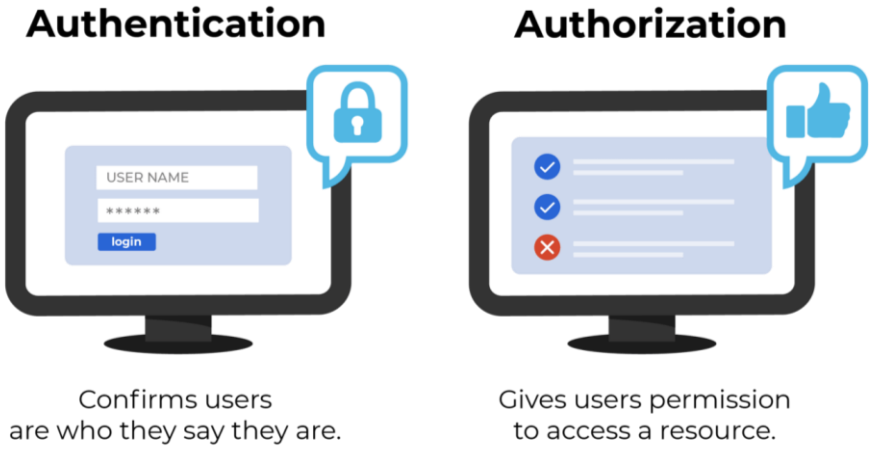
1. **Misstrauen gegenüber allem**: In einem Zero Trust-Netzwerk wird grundsätzlich niemandem oder nichts vertraut. Alle Benutzer, Geräte und Anwendungen werden als potenzielle Sicherheitsrisiken betrachtet.
2. **Minimierung von Berechtigungen**: Benutzer und Geräte erhalten nur die minimal erforderlichen Zugriffsrechte, um ihre Aufgaben zu erfüllen. Überprivilegien werden vermieden.
3. **Kontinuierliche Überprüfung**: Die Identität und der Status von Benutzern und Geräten werden kontinuierlich überwacht und überprüft, auch während einer laufenden Sitzung.
4. **Mikrosegmentierung**: Das Netzwerk wird in kleine, isolierte Bereiche unterteilt, in denen der Datenverkehr streng kontrolliert wird. Dies minimiert die Angriffsfläche und begrenzt die Ausbreitung von Bedrohungen.
5. **Zero Trust Access**: Der Zugriff auf Ressourcen erfolgt auf Basis strenger Authentifizierung und Autorisierung. Jeder Zugriffsversuch wird überprüft, bevor er gewährt wird.

Es wird deutlich, dass Zero Trust eher eine Philosophie als eine Sammlung von Tools ist, das Implementieren dieser Strategie verlangt außer der Nutzung bestimmter Tool Sets auch eine Änderung des Mindsets innerhalb des Unternehmens, mindestens auf der Ebene der Administratoren, besser auf der Ebene aller Nutzer.

Authentifizierung und Autorisierung

Zero Trust, wie der Name schon sagt, geht davon aus, dass der Gegner schon im System ist (Assume Breach) und setzt dieser Annahme die konstante Verifizierung (Always verify) der angegebenen Identität entgegen. Somit wird nicht nur die Identität der Schlüssel zu den verwalteten Ressourcen, sondern vor allem die mit der Identität verknüpfte Berechtigung.

Im klassischen Perimeter Modell werden Rechte – auch erhöhte Rechte – permanent vergeben. Das bedeutet, dass die Rollenzuweisung einmalig erfolgt und dann auch konsequent Bestand hat. Angreifer, denen es gelingt, Zugriff auf diese Rollen zu bekommen, können ungestört ihre Ziele durchsetzen. In modernen Sicherheitsarchitekturen bedeutet Zugangskontrolle immer auch Rechtekontrolle.



Wir müssen also zwischen Authentifizierung (AuthN) und Autorisierung (AuthZ) unterscheiden. Der Unterschied ist im Alltag in den meisten Fällen nicht spürbar.

Authentifizierung

Bei der Authentifizierung geht es darum, wer Sie sind. Ein einfaches Beispiel ist, wenn Sie irgendwo einen Benutzernamen und ein Passwort eingeben. Ein anspruchsvolleres Szenario wäre die Eröffnung eines Kontos, bei der sie ihre Identität durch ihren Personalausweis belegen müssen.

Bei der Authentifizierung wird also überprüft, ob Sie die Person sind, die Sie vorgeben zu sein.

Autorisierung

Bei der Autorisierung geht es darum, was Sie tun dürfen. Ein einfaches Beispiel wäre, dass Sie ein Git-Repository klonen und in dieses pushen dürfen, aber Sie sind nicht berechtigt, Branches in diesem Repository zu löschen. Die Berechtigung muss von einer Instanz erteilt werden, die mehr Rechte hat ("privilegierter" ist) als Sie.

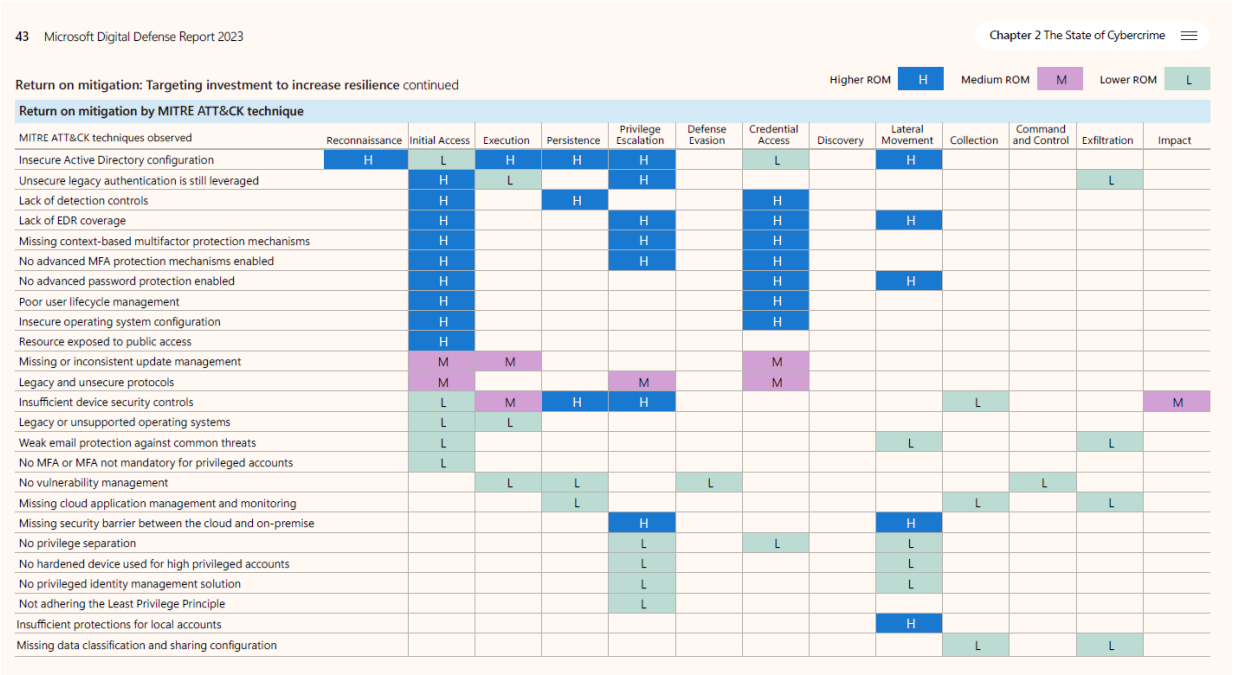
Bei der Autorisierung wird also überprüft, was Sie tun dürfen.

Authentifizierung kann ohne Autorisierung verwendet werden, aber umgekehrt ist dies nicht möglich. Um jemanden oder etwas zu autorisieren - nicht nur natürliche Personen können authentifiziert oder autorisiert werden, sondern auch Entitäten wie Computer, Server, APIs - ist es erforderlich, sich zunächst zu authentifizieren, um zu wissen, ob Zugang gewährt oder verweigert wird (autorisieren). Erst wenn nachweislich bestätigt wird, dass sie die Person sind, die sie vorgeben zu sein, erhalten sie Zugriff im Rahmen ihrer Rechte.

So logisch und einfach das auch klingen mag, in der Realität wird in den meisten Fällen nur die Authentifizierung durchgeführt. Das mag auf historisch gewachsenen Rollen beruhen oder einem generellen Unverständnis moderner Bedrohungsszenarien geschuldet sein; schwache, veraltete oder unzureichende Authentifizierung ohne Autorisierung vor allem bei administrativen (privilegierten) Konten ist eine der Hauptangriffsstellen.

Die nachfolgende Grafik aus dem Microsoft Digital Defense Report 2023 zeigt nicht nur Schwachstellen auf, sondern beschreibt eindrücklich an welchen Stellen schnell ein höherer Schutz (RoM: Return on Mitigation) erreicht werden kann.

Das sind vor allem Maßnahmen in der Zugriffskontrolle, der Kombination aus AuthN & AuthZ.



43 Microsoft Digital Defense Report 2023

Chapter 2 The State of Cybercrime

Return on mitigation: Targeting investment to increase resilience continued

Higher ROM H Medium ROM M Lower ROM L

Return on mitigation by MITRE ATT&CK technique

MITRE ATT&CK techniques observed	Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Insecure Active Directory configuration	H	L	H	H	H		L		H				
Unsecure legacy authentication is still leveraged		H	L		H							L	
Lack of detection controls		H		H			H						
Lack of EDR coverage		H			H		H		H				
Missing context-based multifactor protection mechanisms		H			H		H						
No advanced MFA protection mechanisms enabled		H			H		H						
No advanced password protection enabled		H					H		H				
Poor user lifecycle management		H					H						
Insecure operating system configuration		H					H						
Resource exposed to public access		H											
Missing or inconsistent update management		M	M				M						
Legacy and unsecure protocols		M			M		M						
Insufficient device security controls		L	M	H	H					L			M
Legacy or unsupported operating systems		L	L										
Weak email protection against common threats		L							L			L	
No MFA or MFA not mandatory for privileged accounts		L											
No vulnerability management			L	L		L					L		
Missing cloud application management and monitoring				L						L		L	
Missing security barrier between the cloud and on-premise					H				H				
No privilege separation					L		L		L				
No hardened device used for high privileged accounts					L				L				
No privileged identity management solution					L				L				
Not adhering the Least Privilege Principle					L								
Insufficient protections for local accounts									H				
Missing data classification and sharing configuration										L		L	

Den höchsten Nutzen sehen wir in den Taktiken „Initial Access“, „Privilege Escalation“ und „Credential Access“. Hier kann mit den richtigen Schritten die Angriffsfläche deutlich verkleinert werden, was das Risiko erheblich minimiert.

Verringern der Angriffsfläche

Never Trust.

Always verify.

Assume Breach.

Auf diesen drei Grundsätzen baut ein weiteres Prinzip auf, um die Angriffsfläche zu verringern:

Least Privilege.

Das Prinzip der minimalen Berechtigung verändert radikal die Rollenzuweisung im Vergleich zu den klassischen Berechtigungsmodellen, bei denen einmal zugewiesene Rollen immer und mit vollem Umfang verfügbar sind. Das sind die Felder, die in der Grafik oben mit H markiert sind. Hier kann schnell Schaden vermieden werden – weil mit einfachen Schritten die Einfallstore der Gegner geschlossen werden.

Dem Prinzip des Least Privilege folgend, erhalten alle User – unabhängig von ihrer Funktion – minimale Rechte, im Zweifelsfall nicht mehr als Leserechte. Die alte Prämisse, dass ein Admin IMMER alle Rechte braucht und damit eine immense Sammlung von Berechtigungen auf sich vereint, muss verabschiedet werden. Mit diesem einfachen Schritt können die drei Angriffsvektoren „Initial Access“, „Privilege Escalation“ und „Credential Access“ abgebogen werden. Gegner, deren gestohlene Identität keine Rechte hat und nur mit merklichem Aufwand auf Gegnerseite, welche bekommt, erkennen schnell, dass der Aufwand größer als der Nutzen ist und wenden sich einfacheren Zielen zu.

Böswillige Akteure gehen immer den Weg des geringsten Widerstands, um die Kosten-Nutzen-Rechnung zu erhalten.

Die berechtigte Frage ist, wie gearbeitet werden soll, wenn alle Nutzer nur Leserechte haben.

PIM & PAM

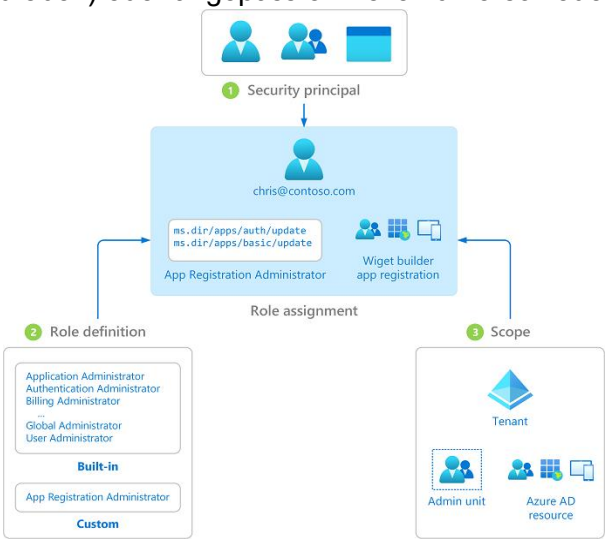
Die Verwaltung der Userrechte kann einfach und unkompliziert über die Rollenbasierte Zugriffskontrolle im Entra ID erfolgen. Microsoft bietet im Standard eine Vielzahl Rollen an, die so granular sind, dass nur bestimmte Handlungsschritte erlaubt sind.

Role	Description	Privileged	Ass...	Type
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	0	Built-in
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED	0	Built-in
Attack Payload Author	Can create attack payloads that an administrator can initiate later.		0	Built-in
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.		0	Built-in
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.		0	Built-in
Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.		0	Built-in
Attribute Definition Administrator	Define and manage the definition of custom security attributes.		0	Built-in
Attribute Definition Reader	Read the definition of custom security attributes.		0	Built-in
Attribute Log Administrator	Read audit logs and configure diagnostic settings for events related to custom security attributes.		0	Built-in
Attribute Log Reader	Read audit logs related to custom security attributes.		0	Built-in

Einige Rollen sind mit dem Label „Privileged“ gekennzeichnet, diese Rollen sollten immer mit Vorsicht ausgewählt werden. Das Verfahren ist ganz einfach.

Schritt 1 fordert der sogenannte Security Principal einen Zugriff an. Das kann ein User / eine Gruppe / oder eine Maschinen-Identität sein.

In Schritt 2 wird die Identität mit der zugewiesenen Rolle abgeglichen. Hier kann zwischen eingebauten Rollen (Bild oben) oder angepassten Rollen unterschieden werden.



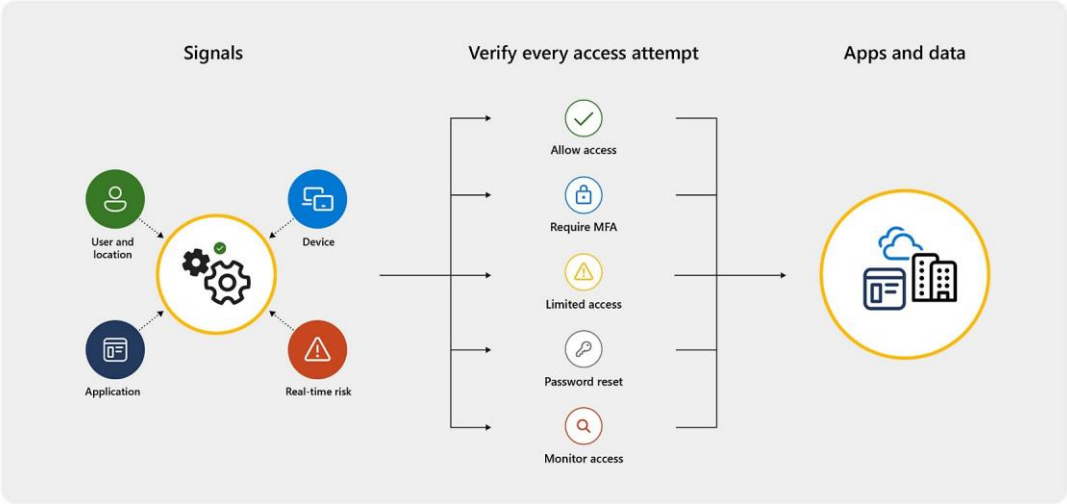
Schritt 3 beschreibt den Umfang (Scope) der Rolle. Rollen können auf Mandantenebenen, Gruppen oder auf ausgewählte Ressourcen zugewiesen werden.

Dieses Prinzip der Rollenvergabe ist zwar deutlich granularer als bei traditionellen Konzepten, ermöglicht es aber weiterhin, diese Rollen 24/7 auszuüben.

In diesem Konstrukt ist der Schadensbereich, der sogenannte „Blast-Radius“, den ein Angreifer verursachen kann, zwar schon eingeschränkt, aber immer noch vorhanden. Ziel muss daher sein, genau diesen „Blast Radius“ so weit einzuschränken, dass selbst bei erfolgreicher Übernahme einer Identität nur minimaler Schaden angerichtet wird. Ein erster Schritt dahin ist der bedingte Zugriff, „Conditional Access“, der Zugriff auf die Rolle also von einer oder mehreren Bedingungen abhängig macht. Im Conditional Access wird die Anmeldung einer Entität auf der Basis vorhandener Signale geprüft. Microsoft erfasst und bewertet 750 Millionen Signale in der Sekunde und kann daher jederzeit Anomalien im

Anmeldeverhalten feststellen. Auf der Grundlage der Informationen (vorherige Anmeldungen, Anmeldeorte, Uhrzeiten, etc…) wird entweder eine Anmeldung nach vorhandenen Richtlinien durchgeführt oder eine Zugangskontrolle durchgesetzt. Nur wenn diese Kontrolle erfolgreich passiert wurde, kann die Autorisierung auf eine vorhandene Rolle erfolgen.

Ein wichtiger Bestandteil sicherer Zugangskontrolle ist die Multi-Faktor-Authentifizierung, mit der wir uns im nächsten Abschnitt beschäftigen werden.



Die Anmeldung wird gegen vorhandene Signale und die Microsoft Machine-Learning Engine für Real-Time-Risk Assessment durchgeführt. Danach kann entweder Zugriff gewährt oder eine wiederholte Kontrolle wie MFA (Multi-Faktor-Authentifizierung), eine Passwort-Erneuerung oder ein nur eingeschränkter Zugriff ermöglicht werden.

Mit diesen Maßnahmen wird dem Gegner eine weitere Möglichkeit genommen, Zugriff auf eine Identität zu erhalten und diese mit erhöhten Rechten zu nutzen.

Speziell das „Upgraden“ einer gestohlenen Identität, um dadurch in übergeordnete Systeme einzudringen, wird als Seitwärts-Bewegung oder „lateral Movement“ bezeichnet. Lateral Movement ist durch Zugriffskontrollen wie Conditional Access oder MFA nicht aufzuhalten, hierfür werden komplexere Lösungen benötigt.

Privileged Access Management

Privileged Access Management (PAM) identifiziert die Personen, Prozesse und Technologien, die privilegierten Zugriff benötigen, und legt die erforderlichen Richtlinien fest. Mit PAM können sämtliche Konten geschützt und Identitätsdiebstahl abgewehrt werden.

PAM unterstützt bei der Verwaltung von Identitäten, damit Angreifer nicht unkontrolliert in Netzwerke eindringen und auf privilegierte Konten zugreifen können. Hinzu kommt der Schutz privilegierter Gruppen, die den Zugriff auf domänengebundene Computer und die Anwendungen auf diesen Computern steuern.

Was bietet PAM?

- Bereitstellen von Just-In-Time-Zugriff auf kritische Ressourcen
- Investigative Überwachung privilegierter Sitzungen
- Analysieren untypischer Aktivitäten in Zusammenhang mit einem privilegierten Konto
- Erfassen von Ereignissen für privilegierte Konten
- Erstellen von Berichten über Benutzerzugriff und Aktivitäten privilegierter Konten

Weitere Anwendungsfälle sind die Automatisierung des Benutzerlebenszyklus (d. h. Konten anlegen, bereitstellen und deaktivieren), die Überwachung und Aufzeichnung von Aktivitäten privilegierter Konten, die Absicherung des Remotezugriffs und die Steuerung des Zugriffs durch Dritte.

Die erfolgreiche Implementierung von Privileged Access Management nutzt einige Best Practices:

- Multi-Faktor-Authentifizierung anfordern
- Sicherheitsmaßnahmen automatisieren
- Endpunktbenutzer entfernen
- Baselines festlegen und Abweichungen überwachen
- Just-In-Time-Zugriff gewähren
- Unbefristeten privilegierten Zugriff vermeiden
- Aktivitätsbasierte Zugriffssteuerung durchführen

Privileged Access Management wird im Bereich der Verwaltung administrativer Konten durch

PIM (Privileged Identity Management) ergänzt. PAM verwendet Tools und Technologien, um den Ressourcenzugriff zu steuern und zu überwachen und basiert auf dem Prinzip der geringsten Rechte (damit Mitarbeitende Just-Enough-Zugriff auf ihre Aufgaben erhalten). Dagegen steuert PIM Administrator- und Superuser-Konten, denen zeitlich begrenzter Zugriff gewährt wird, und schützt diese privilegierten Konten.

Privileged Identity Management erweitert die Funktionalität von PAM um die Möglichkeiten der auditierbaren Zugriffsnachweise, die sowohl im Unternehmen zur regelmäßigen Kontrolle dienen können als auch als Nachweis für Ermittlungsbehörden im Falle eines erfolgreich durchgeführten Angriffs.

Just-in-time und Just-enough-Access

Wenn man über den Blast-Radius spricht, also den Bereich des maximalen Schadens, den ein Angreifer anrichten kann und über das Prinzip des Least-Privilege, dann muss man über die Funktionen Just-in-time und Just-enough-Access sprechen. Die sprechenden Namen lassen schon ahnen, was mit diesen Funktionen gemeint ist, aber ein genaueres Verständnis hilft, diese Funktionen als wichtige Sicherheitsfeatures zu verstehen.

Just-In-Time-Administration adressiert das Problem der Übernahme oder des Angriffs von administrativen Konten in Active Directory und Entra ID. Übernimmt Malware oder ein Hacker ein Admin-Konto, besteht hohe Gefahr für das Netzwerk. Just-In-Time stellt sicher, dass jedes Administrator-Konto nur die Rechte hat, die es aktuell braucht.

Mit Just-In-Time-Administration (JIT) können Unternehmen sicherstellen, dass Administratoren in der Umgebung aktuell nur die Rechte haben, die sie benötigen. Die Administratoren müssen die Rechte beantragen und können diese anschließend für die jeweilige Aufgabe nutzen.

Mit JIT werden den Administratoren administrative Berechtigungen zugewiesen, die nach einiger Zeit automatisch wieder ablaufen. Administratoren sollten nicht ununterbrochen maximale Berechtigungen zur Verwaltung der Umgebung haben.

Trotz der Vorteile von Just-in-Time Access gibt es immer noch Lücken im Sicherheitsansatz. Hier kommt das Konzept des Just-Enough Access (JEA) ins Spiel. Der Fokus von JEA liegt darauf, nicht nur den Zeitraum des Zugriffs zu begrenzen, sondern auch die tatsächlichen Rechte und Privilegien, die ein Benutzer erhält, zu beschränken. Anstatt einem Benutzer vollen Administratorzugriff zu gewähren, ermöglicht es JEA, gezielte und granulare Berechtigungen zuzuweisen, die nur die spezifischen Aufgaben abdecken, die der Benutzer ausführen muss.

Die Vorteile von Just-Enough Access

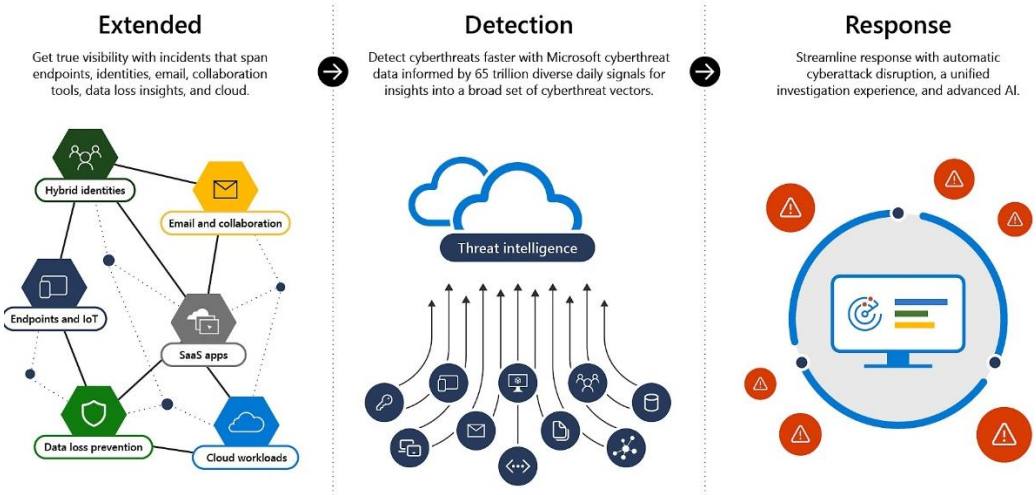
- **Minimierung von Fehlern:** Durch die Begrenzung der Berechtigungen auf das absolute Minimum reduziert JEA das Risiko von unbeabsichtigten Fehlern oder menschlichen Versäumnissen, die zu Sicherheitsverletzungen führen könnten.
- **Stärkere Sicherheit:** Durch die granulare Vergabe von Rechten können Angreifer weniger Schaden anrichten, selbst wenn sie Zugriff auf ein privilegiertes Konto erlangen.
- **Compliance-Anforderungen:** JEA unterstützt Unternehmen dabei, die Anforderungen verschiedener Compliance-Vorschriften einzuhalten, da sie zeigen können, dass nur die notwendigen Zugriffe gewährt wurden.
- **Überwachung und Nachvollziehbarkeit:** JEA ermöglicht eine bessere Überwachung von Benutzeraktivitäten, da nur spezifische Aktionen erlaubt sind, die leichter nachvollzogen werden können.

Mit JIT & JEA wird das Prinzip des Least Privilege im Rahmen der Zero Trust Strategie umgesetzt. Beide Funktionen sind in der Entra ID P2 Lizenz enthalten, ebenso wie PAM & PIM. Viele grundlegende Funktionen wie zum Beispiel MFA sind zwar in der sogenannten „Free“-Version enthalten, um die Kontrolle über die Identitäten zu erhalten und die Umgebung zu schützen, wird das Upgrade auf die Premium Lizenz empfohlen.

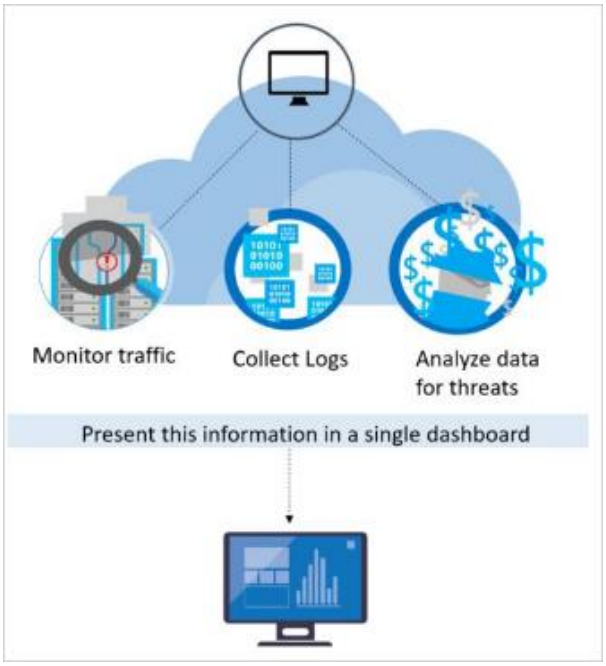
In den Microsoft Office 365 E5 Lizenzen sind die benötigten Premium Features schon enthalten, eine Kontrolle der Lizenzen kann daher viel Geld sparen und möglicherweise eine Menge Sicherheit mit sich bringen.

Maßnahme 3: Extended Detection and Response

Eine Zero Trust Strategie ist nur dann erfolgreich, wenn Angriffsvektoren nicht nur eingeschränkt werden, sondern wenn Bedrohungen als solche erkannt und automatisiert reagiert werden kann.



Erweitert: Echte Sichtbarkeit für Incidents, die Endpunkte, Identitäten, E-Mails, SaaS-Apps, Erkenntnisse zu Datenverlusten und die Cloud umfasst.
Erkennung: Erkennen der Cyberbedrohungen mit Microsoft Cyberbedrohungsdaten, die täglich 65 Billionen Signale auswertet und Einblicke in zahlreiche Cyberbedrohungsvektoren bietet.
Reaktion: Reaktionen mit automatischer Cyberangriffsabwehr, einheitlichen Untersuchungsmethoden und moderner KI beschleunigen.



Microsoft Defender for Cloud und Microsoft Defender für M365 ergeben den Microsoft Defender XDR, eine umfassende Lösung, die nicht nur auf Microsoft Produkte beschränkt ist, sondern die Sicherheitsfeatures sowohl in Azure als auch in Google, AWS oder On-Premises bereitstellt. Eine einheitliche Verwaltungsebene schafft Klarheit und Verlässlichkeit. Die Lösung schützt vor Angriffen auf Geräte, E-Mails, Zusammenarbeit, Identität und Cloud-Apps. Unsere Erkennungs- und Untersuchungsfunktionen bieten eine Single-Pane-of-Glass, um die betriebliche Effizienz erheblich zu verbessern. Microsoft Defender bietet umfassenden Schutz, der durch die Erfassung von Signalen und Interaktion mit den Microsoft Diensten, auf alle Bereiche der IT Umgebung erweitert werden kann.

Microsoft Defender hat mit früheren Versionen des Defender nur noch den Namen gemeinsam. Die gesamte Defender Suite (jetzt Defender XDR) ist eine vollumfängliche Security Lösung, die weit mehr als ein stumpfes Antiviren-Programm ist. Defender nutzt die Informationen, die durch die tägliche Analyse von 750 Millionen Signalen pro Sekunde entstehen und kann dadurch nicht nur umfassend reagieren, sondern auch verlässliche Voraussagen treffen. Mit der Aktivierung des Defender für Cloud wird automatisch Zugriff auf Microsoft 365 Defender gegeben. Somit ist es viel einfacher, Angriffe über Cloudressourcen, Geräte und Identitäten hinweg zu untersuchen. Microsoft 365 Defender bietet eine Übersicht über Angriffe, einschließlich verdächtiger und böswilliger Ereignisse, die in Cloudumgebungen auftreten. Microsoft 365 Defender erreicht dieses Ziel, indem alle Warnungen und Vorfälle, einschließlich Cloudwarnungen und Vorfälle, korreliert werden.

Der Name Defender for Cloud verleitet zu der Annahme, dass es sich hierbei um ein reines Cloudprodukt handelt, was nicht korrekt ist. Die Sicherheitsfeatures des Defender können natürlich auch in On-Premises Umgebungen genutzt werden. Das macht Defender zu einer ganzheitlichen Security Lösung, die es ermöglicht, die gesamte Umgebung unabhängig von der Lokation auf einer Oberfläche zu beobachten.

Eine Security-Strategie ist nur dann wirklich vollständig, wenn der XDR-Part durch ein leistungsfähiges SIEM ergänzt wird. SIEM steht für „Security Incident and Event Management“ ein Tool-Set, das in der Lage ist, Security-Vorfälle nicht nur zu erfassen, sondern auch dementsprechend zu reagieren. Microsoft bietet mit Microsoft Sentinel eine Lösung an, die in den letzten Jahren immer mehr erweitert und zu einem voll integrierten SIEM / SOAR System ausgebaut worden ist. (SOAR steht für „Security Orchestration, Automation and Response“ und bezeichnet Software für das Bedrohungs- und Sicherheitsrisikomanagement, die Reaktion auf Sicherheitsvorfälle und die Automatisierung von Sicherheitsabläufen.) Durch diese Verbindung ist die Priorisierung der von SIEM erstellten Bedrohungen und Warnungen einfacher, indem Incident-Response-Workflows automatisiert werden. Die domänenübergreifende Automatisierung sorgt zudem dafür, dass sich kritische Bedrohungen

zeitnah identifizieren und beseitigen lassen. SOAR spürt reale Bedrohungen in großen Datenmengen auf und beschleunigt so die Beseitigung von Vorfällen.

Die enge Verzahnung von Defender und Sentinel ermöglicht, dass Sicherheitsvorfälle nicht nur schnell erfasst und gemeldet werden, sondern auch automatisiert Reaktionen stattfinden können.

XDR-Dienste helfen die übergreifende Angriffsuntersuchung einheitlich über Endpunkte, Benutzer, Anwendungen, IoT und Workloads hinweg zu unterstützen. So können Ressourcen, geschützt und Bedrohungen wie Ransomware und Phishing abgewehrt werden. Zudem sorgt die automatische Wiederherstellung für die schnelle Reaktion auf Bedrohungen.

SIEM-Dienste nutzt man für die Verwaltung von Sicherheitsabläufen, die Erfassung und Analyse von Daten im gesamten Unternehmen, um Vorfälle zu erkennen, zu untersuchen und Gegenmaßnahmen zu ergreifen.

Die Kombination aus SIEM- und XDR-Lösungen unterstützt eine Strategie, die sowohl umfassende Einblicke in die gesamte digitale Umgebung als auch fundierte Erkenntnisse über bestimmte Bedrohungen liefert.

Microsoft vereinfacht den Security-Aufwand, indem die Vielzahl von Tools, die für den Schutz erforderlich sind, in einer einzigen, effektiven Lösung zusammenfasst werden, die auf KI und Automatisierung basiert. Damit wird ein Hauptproblem der Cybersicherheitsbranche angegangen: die Notwendigkeit, den gesamten digitalen Bestand zu schützen und die SOC-Effizienz durch vereinfachte Tooling-Erfahrung und -Verwaltung zu steigern.

Durch das vereinfachte und zusammengeführte Tooling (Unified Experience), das im Jahr 2024 schrittweise integriert wird, ist die Umsetzung einer Security Strategie noch einfacher geworden. Der Aufbau einer Zero Trust Umgebung, mit den dafür notwendigen Richtlinien und Beschränkungen kann weitgehend Tool unabhängig betrieben werden, auch wenn OOTB Features im Entra ID diesen Weg deutlich vereinfachen und beschleunigen können.

Maßnahme 4: Up to date bleiben

Anbieter von Software reagieren auf Sicherheitslücken in ihrer Software im Normalfall sehr schnell mit Software-Updates (z.B. Security Patches) mit denen diese Lücken schnellstmöglich geschlossen werden.

Allerdings ist es eine Management-Aufgabe, sicherzustellen, dass diese Software-Updates auch sofort nach Verfügbarkeit installiert werden.

Hier bieten Cloud-Lösungen große Vorteile gegenüber On-Premise-Lösungen. Denn im Shared-Responsibility-Modell einer Public Cloud liegt der überwiegende Teil der Verantwortung beim Cloud-Provider. Der Cloud-Anbieter sichert vertraglich zu, dass Security-Patches, wenn verfügbar, sofort installiert werden.

Bei Anwendungssoftware, wie z.B. Office-Software oder Datenbank-Software, ist sicherzustellen, dass eine Version verwendet wird, die noch regelmäßigen Support erhält und damit auch Sicherheits-Updates bekommt.

Maßnahme 5: Daten schützen

Ebenso wie in der „alten, analogen Welt“, gehören auch in der digitalen Jetzt-Zeit keine vertraulichen Daten ans „Schwarze Brett“. Konkret heißt dies, dass alle Informationen, die zur Administration eines IT-Umgebung benötigt werden, in einen digitalen Safe gehören, dessen Schlüssel nur befugte Personen haben.

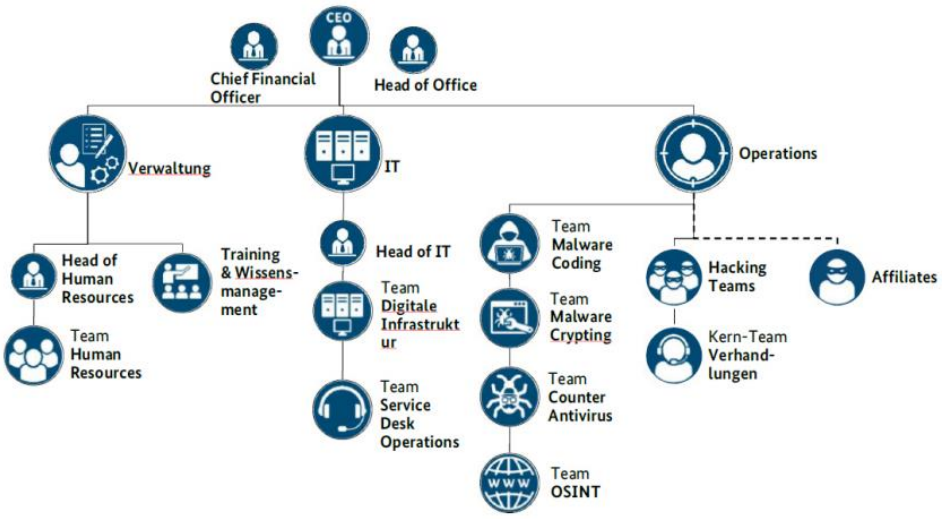
In Azure gibt es hierfür den kostenlosen Service Azure Key Vault. Azure Key Vault sorgt für die sichere Speicherung von Informationen und den Zugriff auf Informationen, die geheim sind bzw. sein sollen, also nur sehr beschränkt zugänglich. Solche Geheimnisse, deren Zugriff streng kontrolliert wird, sind z. B. API-Schlüssel, Kennwörter, Zertifikate oder kryptografische Schlüssel.

Informationen zur Bedrohungslage – wie arbeiten Cyber-Kriminelle?

Auf den vorangegangenen Seiten haben wir erläutert, wie Sie sich und ihre Firma vor Cyberattacken schützen können. Nun wird erklärt, wie diese böswilligen Akteure es schaffen, in die Systeme von Unternehmen einzudringen.

Cybercrime müssen wir als perfekt organisiertes Verbrechen verstehen. Das Bild des Hackers, der allein aus einem Keller heraus wahllos Schaden anrichtet, kann getrost zu den Akten gelegt werden. Wir haben es hier mit Unternehmen zu tun, zu deren Einkommensquelle böswillige Aktionen in IT-Infrastruktur gehören. Diese Unternehmen haben eine strikte Aufgabenteilung und legen größten Wert auf Unsichtbarkeit im „normalen“ Internet. Anhand der Zeitfenster in denen Angriffe passieren und anhand der saisonalen Schwankungen bei Methoden, wie zum Beispiel Phishing, kann man erkennen, dass die Angreifer hauptsächlich zu üblichen Bürozeiten arbeiten und über spezielle Feiertage, wie zum Beispiel Weihnachten die Zahl der Angriffe etwas abnimmt.

In dieser Zeichnung des BKA lassen sich die Organisationsstrukturen eines Unternehmens, das sich auf Ransomware-as-a-Service (RaaS) spezialisiert hat, gut erkennen.



Ransomware verursachte einen Schaden von 10,7 Mrd. Euro in Deutschland.

Die Schadenssumme bleibt für viele Unternehmen existenzbedrohend.

Was ist Ransomware-as-a-Service?

Ransomware-as-a-Service, kurz RaaS, bietet wie andere as-a-Service-Modelle, etwa Software as a Service oder Plattform as a Service, externe IT-Dienstleistungen an, welche an ihre Kunden vermietet werden. Diese müssen die entsprechende Schadsoftware somit nicht selbst entwickeln und bereitstellen.

Ransomware, auch bekannt als Verschlüsselungstrojaner oder Erpressungssoftware, ist ein Schadprogramm, mit welchem Angreifer den Zugriff oder die Nutzung auf Daten oder des gesamten Computersystems des Opfers verhindern können. Dies geschieht etwa durch die Verschlüsselung der Daten auf dem Computer. Zur Entschlüsselung oder Freigabe wird ein entsprechendes Lösegeld gefordert.

Ransomware-as-a-Service zeichnet sich als zukünftiger Trend ab. Sie können somit auf schnelle Art und Weise ein RaaS-Kit erwerben und dann auch direkt eine Attacke mit dieser starten. Gefunden werden, können diese im Darknet.

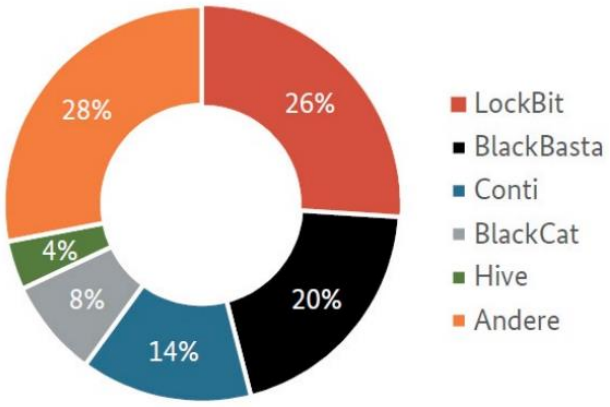
RaaS-Modelle umfassen hierbei verschiedene Umsatzmodelle. Anbieter können beispielsweise eine monatliche Gebühr in Form eines Abos verlangen oder einen Prozentsatz der Gewinne ihrer Kunden einbehalten (Affiliate-Programme). Auch ist eine Mischung aus beiden Modellen oder eine einmalige Lizenzgebühr möglich. Kunden erstellen für den Kauf ein Konto bei dem RaaS-Anbieter, wählen ein entsprechendes Zahlungsmittel (üblicherweise Bitcoin) und können dann die gewünschte Schadsoftware auswählen. Der Leistungsumfang kann je nach Anbieter und gebuchter Dienstleistung unterschiedlich sein und etwa Zugang zu Dokumentationen, 24-Stunden-Support, Communities, Updates oder andere Vorteile umfassen.

Nachdem die Zahlung erfolgt ist, beginnen die Angreifer mit der Verbreitung der Malware und dem Angriff auf das Opfer. Meistens verwenden Ransomware-Angreifer Phishing- oder Social-Engineering-Kampagnen, um die Benutzer zur Ausführung der Malware zu verleiten. Sobald die Malware eingeschleust wurde, wird der Computer des Opfers verschlüsselt und unbrauchbar gemacht, anschließend wird dem Geschädigten eine Nachricht mit Anweisungen über die Lösegeldsendung angezeigt.

RaaS ist genauso wettbewerbsfähig wie jede andere Branche und viele Anbieter vermarkten ihre Dienste aggressiv. RaaS-Anbieter haben Twitter-Konten, Websites, Videoinhalte und andere Marketingmittel. Oft werden Marketingkampagnen durchgeführt, um das Geschäft anzukurbeln. Die meisten RaaS-Tools verfügen auch über Nutzerbewertungen und Community-Foren.

RaaS senkt die Einstiegshürde für diese profitable Form der Internetkriminalität erheblich. Jeder mit einem Computer und einer Internetverbindung kann einen Ransomware-Angriff

durchführen. Die Wahrscheinlichkeit, dass sich die Nutzung von RaaS in den kommenden Jahren zunimmt, ist groß.



Hinzu kommt, dass RaaS nicht teuer ist. Die hier abgebildeten Preise sind die durchschnittlichen Kosten, die im Darknet verlangt werden. Bei einer durchschnittlichen Summe von etwa 4 Millionen Euro bei erfolgreichem Angriff sind das sozusagen Schnäppchen.

Überblick häufig verwendeter Ransomware bei deutschen Zielen

Im BKA durchgeführte Auswertungen zeigen, dass 2022 137 Unternehmen mit Sitz in Deutschland mit der Veröffentlichung ihrer Daten

erpresst wurden. Damit war Deutschland nach den USA und dem Vereinigten Königreich am dritthäufigsten betroffen.

Daten deutscher Geschädigter wurden am häufigsten auf den Seiten der Ransomware-Gruppierungen LockBit, BlackBasta und Conti veröffentlicht.

Service	Preis in US $ (gesamt oder pro Nutzungszeitraum / pro Einheit)	
BankingTrojaner *(Malware, die Bankdaten abgreift)*		
▪ **Desktop-Version**	1.000 - 10.000 $	bei Kauf
▪ **Mobile-Version**	1.000 - 10.000 $	bei Kauf
Bulletproof Hosting *(Siehe QR-Code)*		
▪ **Shared**	5 - 50 $	pro Monat bei Miete
▪ **Dedicated**	12,50 – 3.300 $	pro Monat bei Miete
Counter-AV-Service *(Siehe QR-Code)*	0,15 - 85 $	pro Monat und 300 Scans
Crypting *(Siehe QR-Code)*	0 - 200 $	bei Kauf von einem Crypt
	30 – 2.900 $	Wochen-Abo mit 50 Crypts pro Tag
DDoS-as-a-Service *(Services zum Durchführen von DDoS-Angriffen)*	50 – 2.600 $	pro Monat bei Miete
Infection-on-Demand *(Phishing-Services o.ä.)*	100 – 600 $	pro Monat
Mining Bots *(Malware, die auf infizierten Endgeräten Kryptowährung „schürft")*	50 – 300 $	pro Monat bei Miete
	500 – 3.500 $	bei Kauf
RAT (Remote Administration Tool) *(Programm, dass Fernzugriffe auf ein Zielsystem ermöglicht)*	3 - 530 $	pro Monat bei Miete
	40 - 8.000 $	bei Kauf
Stealer Logs *(Protokolldateien ausgespähter Daten eines infizierten Systems, z.B. Zugangsdaten)*	0,01 - 40 $	pro Stück
	400 – 3.000 $	pro Monat für Abonnement

LockBit

Aktivität: Seit 2019

Zielspektrum: Primär KMU

Relevanz: Eine der aktivsten RaaS-Gruppierungen weltweit.

Besonderheiten: Im Juni 2022 veröffentlichten die Akteure hinter LockBit Version 3.0 ihrer Ransomware sowie eine aktualisierte DLS. Ein Novum stellt dabei unter anderem das angebotene „Bug Bounty Programm" dar, im Rahmen dessen Hinweise auf Schwachstellen in der Ransomware LockBit 3.0 mit einer Geldprämie entlohnt werden.

Conti

Aktivität: 2020 – 2022

Zielspektrum: Big Game, einschl. Gesundheitswesen

Relevanz: Bis zur Auflösung eine der aktivsten RaaS-Gruppierungen weltweit.

Besonderheiten: Die Akteure hinter der Malware Conti (alias Wizard Spider) werden auch mit der Ransomware Ryuk in Verbindung gebracht. Im Zuge des Russland-Ukraine-Kriegs wurden interne Chats und Teile des Conti-Quellcodes geleakt. Dies hatte die Abschaltung der Conti-Infrastruktur zur Folge. Es ist davon auszugehen, dass die Akteure unter neuem Namen weiterhin aktiv sind.

BlackBasta

Aktivität: Seit 2022

Zielspektrum: Kein spezifischer Zieltypus erkennbar

Relevanz: International ist Deutschland am zweithäufigsten von Angriffen mit BlackBasta betroffen.

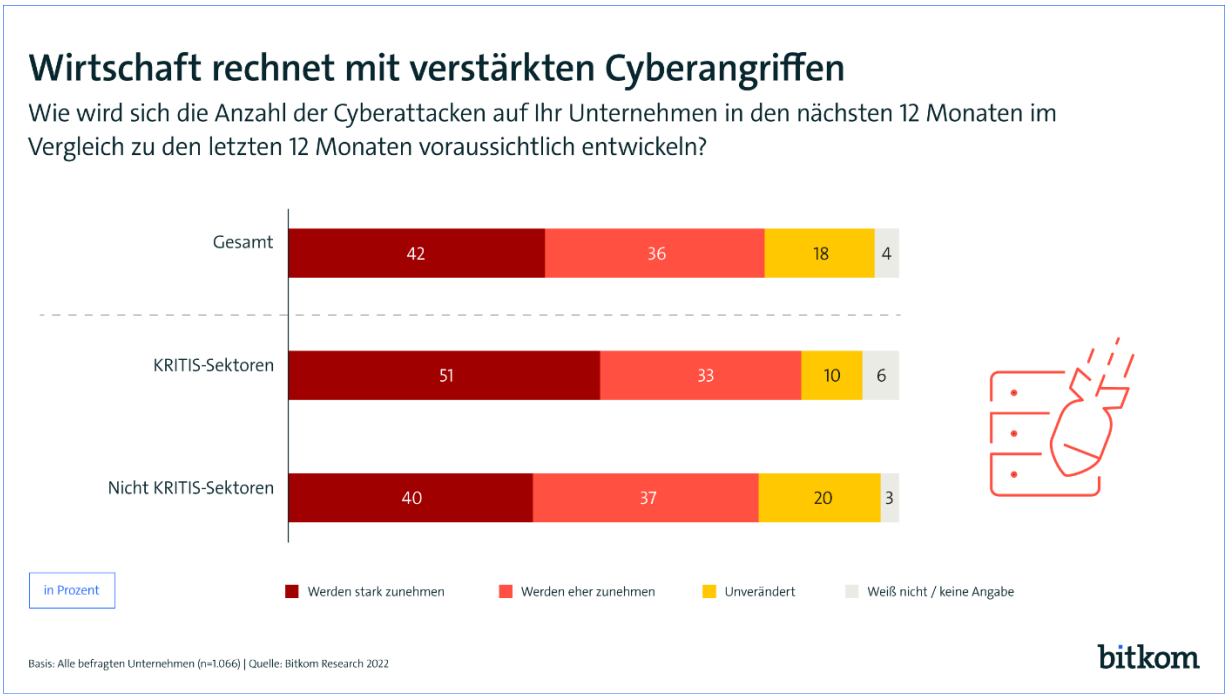
Besonderheiten: Trotz des kurzen Aktivitätszeitraums hat sich BlackBasta bereits international und vor allem in Bezug auf Deutschland zu einer der aktivsten RaaS-Gruppierungen entwickelt. Es ist davon auszugehen, dass es sich bei den Akteuren hinter BlackBasta um erfahrene Cyberkriminelle handelt.

Eine unvollständige Übersicht erfolgreicher Angriffe im vierten Quartal 2023

Unternehmen	Wann	Was
Katholische Hospitalvereinigung Ostwestfalen	24. Dezember 23	Ransomware (LockBit 3.0)
Allgaier Automotive	Dezember 2023	Ransomware
Erfo Bekleidungswerk	Dezember 2023	Ransomware
KaDeWe	November 2023	Ransomware
Südwestfalen IT	Oktober 2023	Ransomware
Motel One	Oktober 2023	Ransomware
Häffner	Oktober 2023	Ransomware
Hochsauerland Wasser, Hochsauerland Energie	September/Oktober2023	Ransomware

Auf der interaktiven Karte der Konbriefing wird das Ausmaß der Angriffe deutlich dargestellt. (**https://konbriefing.com/de-topics/hackerangriff-deutschland.html**)

Einschätzung der Bedrohungslage deutscher Unternehmen



Wie bekommen die Angreifer Zugriff auf die Systeme?

Der Großteil der deutschen Unternehmen setzt immer noch auf eine schwache Authentifizierung in der Verbindung Benutzername und Passwort. Das beliebteste Passwort der Deutschen im Jahr 2023 war »123456789«, hatte also immerhin drei Ziffern mehr als im Vorjahr, wie das Hasso-Plattner-Institut (HPI) in Potsdam am Dienstag mitteilte. Es ist damit minimal weniger unsicher, aber eben alles andere als sicher. Die fünf vorderen Plätze der Rangliste werden demnach bis auf die Ausnahme »hallo« auf Platz drei allesamt von schwachen Ziffernreihen belegt.

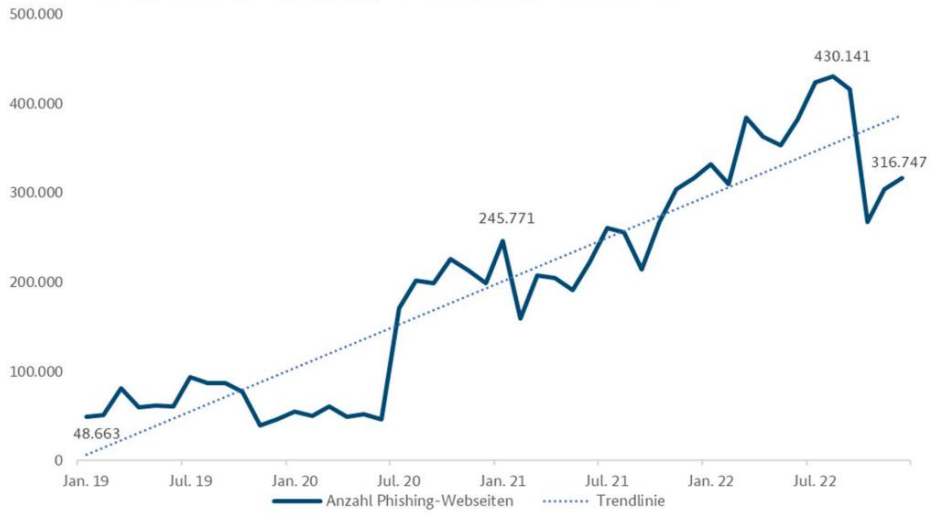
Selbst komplexere Passwörter bieten keinen vollständigen Schutz. Diese Kombinationen können für sehr wenig Geld (wenige hundert Dollar für viele Millionen Paare) im Darknet erworben werden. Sobald ein Angreifer im Besitz dieser Informationen ist, benötigt er keinen Aufwand mehr, um sich Zugang zu den Systemen zu verschaffen.

Phishing wächst kontinuierlich.

Noch viel einfacher wird es für den Angreifer, wenn er die Informationen direkt vom Opfer zur Verfügung gestellt bekommt. So kann der direkte Weg zu administrativen Konten ermöglicht werden, die viel mehr Rechte haben. Die Kosten-Nutzen-Rechnung wird effizienter.

Phishing ist und bleibt einer der beliebtesten Eintrittsvektoren zur Distribution von Malware und dem Abgriff von Zugangsdaten.

Folgende Grafik zeigt Entwicklungen im globalen Phishing-Aufkommen:

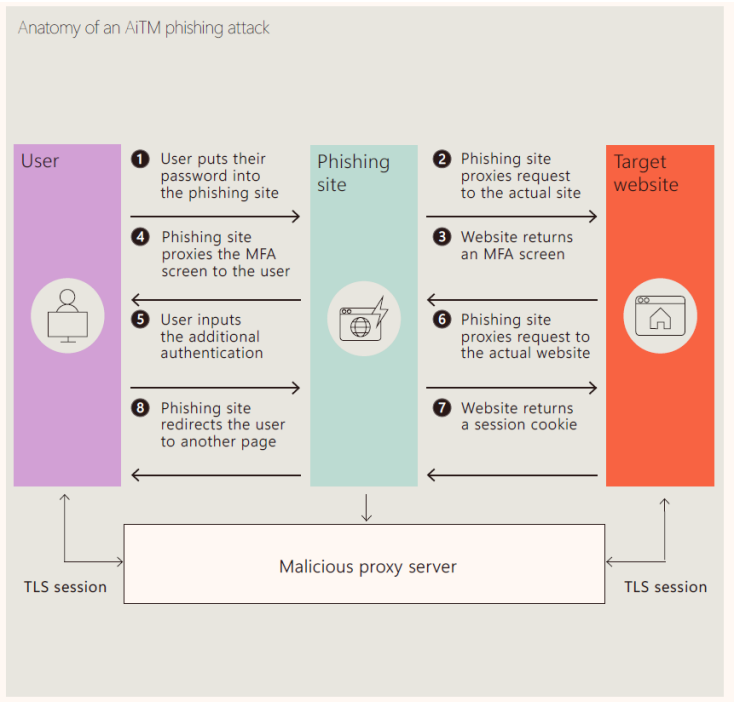


Der Knick im Juli 2023 zeigt einen Einbruch in der Phishing Aktivität, der auf einen erfolgreichen Zugriff der Sicherheitsbehörden zurückzuführen ist. Der steigende Trend über die vergangenen drei Jahre bleibt jedoch intakt.

Die Technik des Phishings wird immer ausgefeilter, die Angreifer sind mittlerweile in der Lage, zielgenaue („targeted“) Mails zu erstellen, die auch auf einen zweiten Blick nicht als böswillig auffallen. Hinzu kommt die Nutzung von Messenger-Diensten, SMS oder Anrufen, immer mit dem Ziel, persönliche, sensible Informationen zu erlangen.

Die folgende Grafik zeigt wie sogenannte „Adversary-in-the-middle“ Attacken ablaufen, bei denen ein Angreifer einen legitimen Anmeldeprozess nutzt, um Daten zu erhalten.

Diese Art der Angriffe, die Standard Multifaktor Authentifizierungen aushebeln, um so ihre Angriffsziele zu erreichen, sind seit 2021 stark zunehmend.



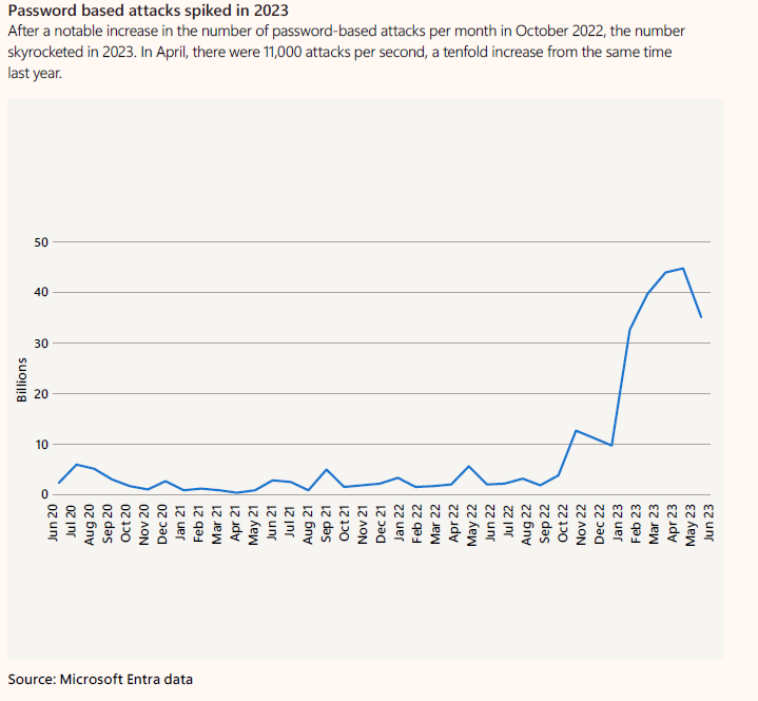
Bei einem Adversary-in-the-middle - Phishing-Angriff wird ein Reverse-Proxy Proxy-Server zwischen dem Ziel und einer legitimen

Anmeldeseite genutzt. Reverse-Proxy-Server sitzen zwischen einem Client, z. B. einem Webbrowser, und einem Webserver und leiten Informationen und Anfragen zwischen dem Client und dem Server weiter.

Die Zielperson gibt unwissentlich ihre Anmeldedaten über den Proxy ein, was eine MFA-Aufforderung auf ihrem mobilen Gerät auslöst. Nachdem der Benutzer den Authentifizierungscode eingegeben hat, erhält der Proxy die Täuschung, indem er nachfolgende MFA-Bildschirme, die die Eingaben des Benutzers ohne dessen Wissen weiterleitet und damit den Zugriff auf das Konto gewährt.

Hieran kann man gut erkennen, warum Authentifizierung allein nicht ausreicht, sondern immer durch Autorisierung ergänzt werden sollte.

Die Zahl der Angriffe auf Identitäten ist drastisch gestiegen.



Warum werden Identitäten gestohlen?

Identitäten bieten einem Angreifer die Möglichkeit sämtliche Hürden zu umgehen, die „klassische“ Security normalerweise bereithält. Viele, viele Jahre lang waren IT-Umgebungen aufgebaut wie mittelalterliche Burgen. Die Firewall riegelte Netzwerke von außen ab, Verbindungen nach außen wurden über granulare Freigaben erreicht. Security war statisch. Solange die Firewall sicher war, solange die Burg gesichert wurde, war alles in Ordnung.

Aus dieser Zeit kommt das Verständnis – oder besser Unverständnis – für Security Budgets. Da die Sicherheit von der Firewall abhing und diese ja schon bezahlt worden war, erschien jede weitere Maßnahme als unnötiger Kostenpunkt. Diese Zeiten sind lange vorbei und spätestens seit der Corona Pandemie sollte den meisten Unternehmen klar geworden sein, dass diese Herangehensweise nicht mehr zielführend ist.

Die Netzwerke, der sogenannte Perimeter, sind kein Teil mehr der Angriffskette. Sie sind Hürden, die den Fortschritt des Angriffs verlangsamen – aber nicht unbedingt aufhalten.

Sobald ein Angreifer eine Identität erobert hat, steht ihm auch keine Firewall mehr im Weg. Ganz im Gegenteil, sobald er seine gestohlene Identität um die notwendigen Rechte erweitert hat, kann er die Firewall so einstellen, dass sie ihm für jede weitere Handlung nicht mehr im Weg steht.

Quellen:

Pressemitteilung BKA

Bitkom Umfrage

https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.pdf?__blob=publicationFile&v=5

https://www.csoonline.com/de/a/diese-unternehmen-hat-s-schon-erwischt,3674038

https://konbriefing.com/de-topics/cyberangriff-2023-sit-suedwestfalen-it. html

https://konbriefing.com/de-topics/hackerangriff-deutschland.html
https://de.wikipedia.org/wiki/Ransomware-as-a-Service

https://sec.hpi.de/ilc/

https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

https://www.microsoft.com/de-at/security/security-insider/microsoft-digital-defense-report-2023

https://attack.mitre.org/

https://de.wikipedia.org/wiki/Zero_Trust_Security

https://learn.microsoft.com/de-de/entra/identity/role-based-access-control/permissions-reference