



controlware

Controlware Threat Report

Daten, Trends und Empfehlungen
zur aktuellen Cybersicherheitslage
2025



Controlware Threat Report

Daten, Trends und Empfehlungen zur aktuellen Cybersicherheitslage

1. Einleitung

Ein eskalierendes Bedrohungsumfeld

In den vergangenen Jahren hat sich die Cyberkriminalität deutlich gewandelt: Statt einzelner, opportunistischer Angriffe dominieren heute hochspezialisierte und industrialisierte Kampagnen. „Phishing-as-a-Service“, Adversary-in-the-Middle-(AiTM)-Angriffe und fortschrittliche Social-Engineering-Techniken wie ClickFix zeigen, wie leicht klassische Schutzmechanismen wie Multi-Faktor-Authentifizierung umgangen werden können. Gleichzeitig verbreiten sich verstärkt hochentwickelte Malware-Familien – darunter mobile Spyware und Kryptowährungs-Trojaner – über komplexe Infektionsketten, die zunehmend Cloud-Dienste und Lieferketten ausnutzen.

Parallel dazu haben staatlich unterstützte Angreifer ihre Aktivitäten intensiviert. Sie nutzen Zero-Day-Schwachstellen oder offene bekannte Verwundbarkeiten in weit verbreiteten Plattformen aus, um Behörden, kritische Infrastrukturen und Unternehmen anzugreifen. Die Zeiten der Zurückhaltung sind vorbei: Angriffe zeichnen sich durch höhere Aggressivität, größere

Hartnäckigkeit und verstärkte politische Zielsetzungen aus.

Die Rolle der Künstlichen Intelligenz

Künstliche Intelligenz (KI) verstärkt diese Dynamik auf beiden Seiten. Für Angreifer senkt KI die Einstiegshürden, indem sie Aufklärung, Phishing und initiale Zugriffsphasen automatisiert. Weniger erfahrene Gruppen können dadurch Kampagnen durchführen, die bisher nur fortgeschrittenen Akteuren vorbehalten waren. Gleichzeitig setzen gut ausgestattete Bedrohungsakteure KI ein, um gezielte und adaptive Angriffe zu entwickeln – schneller und in größerem Umfang als je zuvor.

Auch Verteidiger nutzen KI in Endpoint Detection and Response (EDR)-, Extended Detection and Response (XDR)- und Security Information and Event Management (SIEM)-Systemen, um Bedrohungen schneller zu erkennen und den Mangel an Analysten abzufedern. Dennoch droht die Geschwindigkeit offensiver Innovationen die defensive Nutzung zu überholen, wenn Organisationen weiterhin primär reaktiv handeln.

EXECUTIVE SUMMARY

Die Cybersicherheitslandschaft befindet sich weltweit und insbesondere im DACH-Raum in einem fundamentalen Wandel. Angreifer agieren zunehmend professionell, kreativ und ressourcenstark. Neue technologische Möglichkeiten, staatlich unterstützte Cyberaktivitäten sowie ein akuter Fachkräftemangel führen zu systemischen Risiken für Unternehmen, öffentliche Institutionen und kritische Infrastrukturen.

Auswirkungen auf den DACH-Markt

Für den DACH-Raum sind die Risiken besonders hoch. Die starke industrielle Basis, die komplexen Lieferketten und der hohe Digitalisierungsgrad machen Unternehmen zu attraktiven Zielen. Gleichzeitig stehen viele Organisationen vor der doppelten Herausforderung, steigende regulatorische Anforderungen unter EU- und nationalem Recht zu erfüllen sowie gleichzeitig mit einem chronischen Mangel an Cybersecurity-Fachkräften umzugehen.

„Der Übergang zu integrierten, Intelligence-basierten und kontinuierlich adaptiven Verteidigungsmodellen ist daher keine Option, sondern eine zwingende Notwendigkeit, um die Resilienz in einer digitalen Wirtschaft sicherzustellen – in einer Welt, in der ‚Business as usual‘ nicht mehr funktioniert.“

Eine wachsende Angriffsfläche, kombiniert mit Angreifern, die KI und staatliche Ressourcen nutzen, schafft ein Risikoumfeld, in dem traditionelle Perimetersicherheit und punktuelle Schutzmaßnahmen nicht mehr ausreichen.

Der Weg nach vorn

Entscheidungsträger sollten Cybersicherheit als strategische Priorität begreifen. Dazu gehören:

- **Ganzheitliche Verteidigungsstrategien**, die technische Maßnahmen, Benutzeraufklärung und kontinuierliche Incident Response integrieren.
- **Resiliente Architekturen** wie Zero Trust und Conditional Access, um die Auswirkungen gestohlener Zugangsdaten oder umgangener MFA zu minimieren.
- **Kontinuierliche Überwachung und Erkennung**, die KI verantwortungsvoll nutzt, um automatisierte Angriffe abzuwehren.
- **Investitionen in die Resilienz der Belegschaft**, damit Mitarbeitende sensibilisiert sind und Manipulationsversuche erkennen können.

Fazit

Die aktuelle Bedrohungslage ist eindeutig: KI-beschleunigte Angriffe, staatlich orchestrierte Akteure und der anhaltende Fachkräftemangel schaffen systemische Risiken. Der Übergang zu integrierten, Intelligence-basierten und kontinuierlich adaptiven Verteidigungsmodellen ist daher keine Option, sondern eine zwingende Notwendigkeit, um die Resilienz in einer digitalen Wirtschaft sicherzustellen – in einer Welt, in der ‚Business as usual‘ nicht mehr funktioniert.

Vor diesem Hintergrund lohnt ein genauer Blick auf die aktuelle Bedrohungslandschaft

2. Thread Landscape

Aktuelle Trends und Methoden

Im aktuellen Bedrohungsumfeld setzen Cyberkriminelle verstärkt auf Social Engineering, maßgeschneiderte Phishing-Kampagnen und den Missbrauch von legitimer Infrastruktur, um klassische Sicherheitsmechanismen zu umgehen. Besonders auffällig ist der Trend, bestehende Schutzmaßnahmen wie die Zwei-Faktor-Authentifizierung, insbesondere im Kontext von Hyperscaler-basierten Infrastruk-

turen, gezielt auszuhebeln und gleichzeitig neue Wege zur Ausführung von Schadcode auszunutzen.

Methoden wie ClickFix zeigen, wie einfach Nutzer durch vermeintlich harmlose Aufforderungen zur Ausführung von Schadcode verleitet werden können. Parallel dazu bieten „Phishing-as-a-Service“-Plattformen wie Salty 2FA Angreifern die Möglichkeit, 2FA-Schutz zuverlässig zu umgehen. Auch sogenannte „Adversary-in-the-Middle“-Angriffe (AiTM), die gezielt auf das Abfangen von Authentifizierungsprozessen und die Umgehung von Zwei-Faktor-Mechanismen abzielen, gewinnen an Bedeutung. Im vorliegenden Bericht werfen wir daher einen genaueren Blick auf die ClickFix-Technik sowie auf AiTM-Methoden, die insbesondere im Kontext von Phishing-Kampagnen eine zentrale Rolle spielen.

Schadsoftware wie der Efimer Trojaner zielt verstärkt auf Kryptowährungen, verbreitet sich über kompromittierte Webseiten und E-Mails und bleibt durch den Einsatz von Tor-Kommunikation schwer nachverfolgbar. Gleichzeitig nehmen komplexere Infektionsketten, etwa über Cloud-Infrastrukturen oder Supply-Chain-Angriffe, weiter zu.

Staatlich unterstützte Angreifer-Gruppen nutzen zudem Zero-Day-Lücken in weit verbreiteten Platt-

„Wir erwarten, dass der Einsatz von Künstlicher Intelligenz (KI) sowohl die Anzahl als auch die Komplexität von Cyberangriffen deutlich erhöhen wird. KI ermöglicht es weniger erfahrenen Angreifergruppen, auf Angriffstechniken zuzugreifen, die bislang außerhalb ihrer Fähigkeiten lagen.“

formen wie Microsoft SharePoint, um Zugang zu Behörden, kritischer Infrastruktur und Unternehmen weltweit zu erlangen. Diese Angriffe sind oft hochgradig ausgefeilt und kombinieren mehrere Schwachstellen, um Schadcode erfolgreich auszuführen.

Auch mobile Bedrohungen rücken zunehmend in den Fokus: Mit Spy-Note wurde eine besonders ausgefeilte Android-Spyware entdeckt, die sich als legitime App tarnt und über erweiterte Systemrechte sensible Daten abgreift. Damit wird die Sicherheit mobiler Endgeräte zu einem zentralen Thema in der aktuellen Bedrohungslage. Dies gilt insbesondere im Zusammenhang mit BYOD und Zwei-Faktor-Authenticator-Apps auf potenziell kompromittierten mobilen Endgeräten.

Fazit und Ausblick

Die Bedrohungslandschaft ist durch eine hohe Professionalisierung und Diversifizierung geprägt. Angreifer kombinieren technische Exploits mit menschlicher Manipulation, um Sicherheitsmechanismen systematisch zu umgehen. Für Unternehmen bedeutet dies, dass reine Perimeter-Sicherheit nicht mehr ausreicht – entscheidend sind ein ganzheitliches Sicherheitskonzept, kontinuierliche

Überwachung und die Sensibilisierung der Mitarbeitenden.

Wir erwarten, dass der Einsatz von Künstlicher Intelligenz (KI) sowohl die Anzahl als auch die Komplexität von Cyberangriffen deutlich erhöhen wird. KI ermöglicht es weniger erfahrenen Angreifergruppen, auf Angriffstechniken zuzugreifen, die bislang außerhalb ihrer Fähigkeiten lagen. Gleichzeitig werden fortgeschrittene Akteure KI nutzen, um noch ausgefeiltere und gezieltere Angriffe durchzuführen. Anthropic (das Unternehmen hinter Claude) hat beobachtet, dass Akteure KI nicht nur nutzen, um fortgeschrittene Techniken zu entwickeln, sondern diese direkt durch KI ausführen zu lassen. KI wird damit direkt zum Akteur der maliziösen Aktionen.

Darüber hinaus ist zu erwarten, dass die Anzahl entdeckter und ausgenutzter Schwachstellen steigt, da KI sowohl bei der Identifikation als auch bei der Ausnutzung von Sicherheitslücken eingesetzt werden kann bzw. wird.

Auf der Verteidigerseite nutzen moderne Sicherheitslösungen – etwa die von Controlware eingesetzten Endpoint bzw. Extended Detection and Response Systeme – ebenfalls KI, um Angriffe frühzeitig zu erkennen und erfolgreich abzuwehren.

3. Detektionsstatistiken

Auswertung nach Sektoren und Techniken

Im Rahmen der Controlware Cyber Defense Services ermitteln wir Statistiken zur Bedrohungslage unterschiedlicher Sektoren unter Berücksichtigung der Kritikalität der Angriffe (Risikoprofil) sowie die von den Angreifern genutzten Techniken (MITRE ATT&CK).

Wir achten in diesem Zusammenhang insbesondere auf die eingesetzten Techniken, da es zwar viele unterschiedlich motivierte Angreifergruppen gibt, diese sich aber in den meisten Fällen einer Kombination aus den immer gleichen Techniken bedienen.

Zu berücksichtigen ist, dass das Controlware Cyber Defense Center diese Angriffsversuche unabhängig vom Schweregrad sowie den eingesetzten Techniken grundsätzlich abwehrt. Spätere Phasen mit höherem Impact erreichen Angreifer nach unserer Analyse insbesondere dann, wenn primär klassische, ausschließlich Log-basierte Sicherheitstechnologie (SIEM) ohne Verfügbarkeit granularer Host-Telemetrie-Daten, wie sie von EDR/XDR-Systemen zur Verfügung gestellt werden, eingesetzt wird.

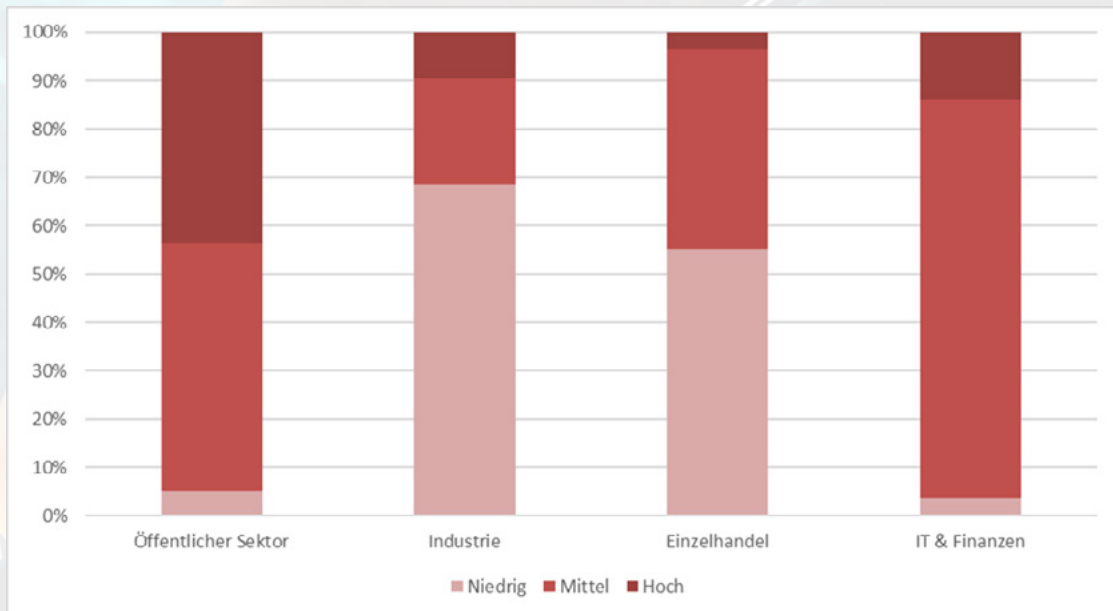


Abbildung 1: Angriffe bezogen auf Sektor und Kritikalität

Die Auswertung der Statistik zeigt deutlich, dass die Bedrohungslage durch Cyber-Incidents stark vom jeweiligen Sektor abhängt und sich die Schwere der Vorfälle branchenspezifisch unterscheidet. Besonders im **Öffentlichen Sektor** ist auffällig, dass der Anteil an mittleren und schweren Incidents dominiert. Dies spiegelt die Realität wider, die auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt. Behörden und öffentliche Einrichtungen geraten zunehmend ins Visier staatlich unterstützter Angriffe, Ransomware-Kampagnen und Cyber-Spionage. Da hier oft kritische Infrastrukturen oder sensible Daten betroffen sind, haben Vorfälle in diesem Bereich ein besonders hohes Schadenspotenzial, dies erklärt den hohen Schweregrad.

In der **Industriebranche** treten Vorfälle überwiegend mit niedrigem Schweregrad auf. Viele Vorfälle werden hier frühzeitig erkannt oder bleiben auf kleinere Störungen beschränkt. Diese Interpretation deckt sich mit aktuellen Beobachtungen, wonach Angriffe auf Produktions-IT und vernetzte Systeme zwar eine wachsende Gefahr darstellen, bisher aber noch vergleichsweise selten in katastrophale Ausfälle münden.

Der **Einzelhandel** nimmt eine Mittelstellung ein. Vorfälle verteilen sich relativ gleichmäßig zwischen Vor-

fällen mit niedrigem und mittlerem Schweregrad, mit einem geringen, aber nicht zu vernachlässigenden Anteil an schwerwiegenden Incidents. Diese können erheblichen finanziellen Schaden nach sich ziehen, erreichen aber vergleichsweise seltener die Tragweite systemkritischer Attacken wie im öffentlichen Sektor oder bei Finanzinstituten.

Die Statistik weist im **Bereich IT & Finanzen** einen überdurchschnittlich hohen Anteil an mittleren Vorfällen auf, ergänzt durch einige hochkritische Incidents. Dies deckt sich mit Analysen der europäischen Cybersicherheitsbehörde ENISA, die für diesen Sektor eine hohe Angriffintensität durch DDoS, Ransomware, Datenlecks und Supply-Chain-Angriffe dokumentiert. Banken, Versicherungen und IT-Dienstleister unterliegen strengen regulatorischen Anforderungen und verfügen über starke Sicherheitsmaßnahmen, was dazu führt, dass viele Angriffe im mittleren Bereich bleiben. Gleichzeitig zeigt der beachtliche Anteil schwerer Incidents, dass trotz hoher Sicherheitsstandards kein vollständiger Schutz möglich ist und die Branche weiterhin ein bevorzugtes Ziel für Angreifer bleibt.

Insgesamt verdeutlicht die Kombination aus Detektionsstatistik und kontextbezogenen Threat-Intel-Infor-

mationen, dass sich Cyberbedrohungen je nach Branche unterschiedlich manifestieren. Während der öffentliche Sektor und die Finanzindustrie stark von schwereren Angriffen betroffen sind, bleiben viele Vorfälle in der Industrie und im Einzelhandel bisher von niedriger oder mittlerer Schwere. Dennoch deuten aktuelle Entwicklungen darauf hin, dass gerade Industrie und Handel in den kommenden Jahren stärker von kritischen Angriffen betroffen sein könnten, wenn Sicherheitsstrategien nicht entsprechend angepasst werden. Dies ist primär abhängig von der Motivation der Angreifer. Diese reicht in der Regel von Cybercrime wie z.B. Ransomware bis zu staatlicher / politischer Motivation.

In **allen Sektoren** fällt auf, dass Lateral Movement (laterale Bewegung innerhalb eines Netzwerks) und Discovery (Aufspüren und Erkunden von Systemen und Netzwerken) zu den stärksten Segmenten gehören. Ebenfalls prominent sind Initial Access (erster Zugriff), Execution (Ausführung von Code), Privilege Escalation (Rechteauserweiterung) sowie Credential Access. Weniger stark ausgeprägt sind Taktiken wie Resource Development oder Impact in manchen Sektoren. So weist beispielsweise der Öffentliche Sektor eine vergleichsweise hohe Nutzung von Persistence-Techniken auf.

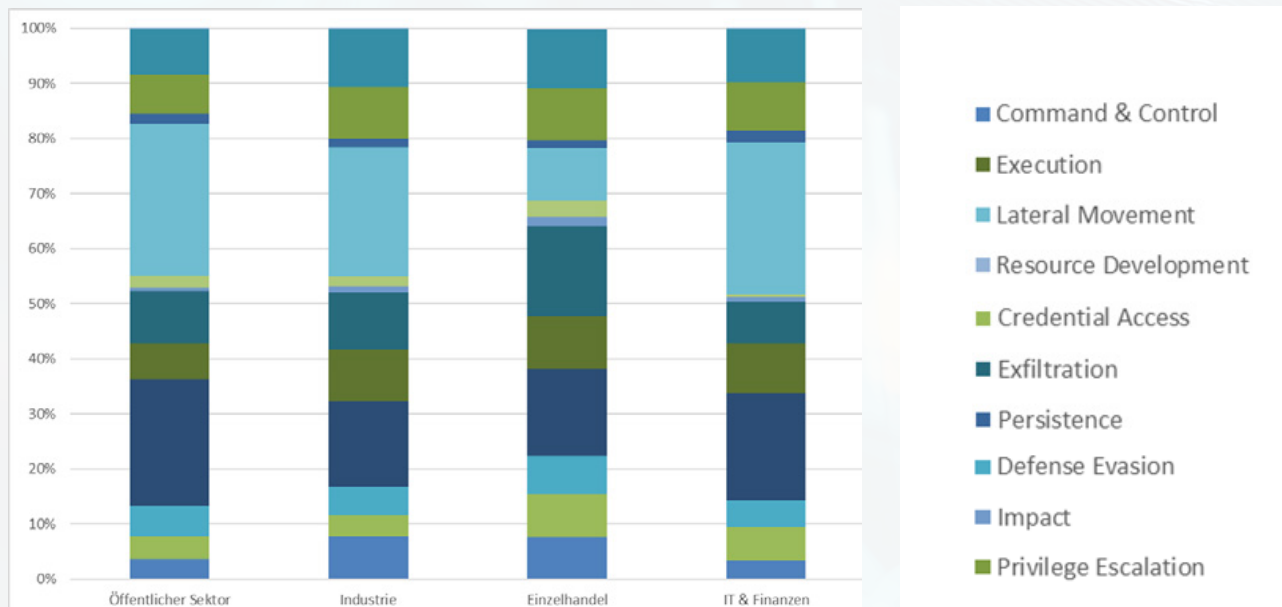


Abbildung 2: Angriffe bezogen auf Sektor und Technik (MITRE ATT&CK)

niken auf. IT & Finanzen sind stark von Credential Access und Command & Control betroffen. Der Einzelhandel zeigt ein relativ großes Segment bei Impact bzw. Exfiltration im Vergleich zur Industrie.

Aus unseren Beobachtungen ergibt sich folgendes Bild im Bereich DACH:

Lateral Movement und Discovery als Schlüsselphasen moderner Angriffe

Die Daten bestätigen, was viele Threat-Intelligence-Reports zeigen: Angreifer nutzen nach dem Erstzugang häufig Techniken, um sich im Netzwerk umzuschauen („Discovery“) und dann lateral zu bewegen, um ihre Reichweite zu vergrößern.

Erstzugriff und Credential Access bleiben kritische Einstiegspunkte

Unsere Statistik zeigt einen hohen Anteil von Credential Access und Initial Access. Auch Threat-Intel-Daten bestätigen, dass Phishing, Ausnutzung öffentlicher Dienste, gestohlene Zugangsdaten etc. nach wie vor zu den häufigsten Methoden gehören, über die Angreifer Zugriff auf Systeme erlangen.

Branchenabhängige Unterschiede in Technikpräferenzen

Im **Öffentlichen Sektor** sind Techniken wie Persistence und Command & Control stärker ausgeprägt. Dies unterstützt Informationen, wonach Behörden bzw. KRITIS-Organisationen oft gezielt langfristig infiltriert werden, z. B. um Informationen zu erlangen oder kritische Infrastruktur zu beobachten und zu manipulieren.

Empfehlungen:

- Ausbau von **Threat Hunting** und kontinuierlichem Monitoring, insbesondere auf verdächtige C2-Kommunikation.
- Stärkung von **Endpoint Detection & Response (EDR/XDR)**, um Persistence-Techniken frühzeitig zu erkennen.
- Härtung der Systeme durch **Zero-Trust-Architekturen** und Micro-Segmentierung.
- Orientierung an BSI-Empfehlungen für KRITIS-Betreiber

Im Sektor **IT & Finanzen** sehen wir große Anteile bei Credential Access, Command & Control und Exfiltration. Dies stimmt mit dem Risikoprofil dieser Branchen überein.

Empfehlungen:

- **Multi-Faktor-Authentifizierung (MFA)** als Pflicht in allen kritischen Systemen.
- Einsatz von **EDR/XDR-Technologie** kombiniert mit KI-basierten Anomalieerkennungen auf Basis der Data Lakes, welche zur Korrelation genutzt werden.
- Starke **Kontrollen für Datenflüsse** (z. B. zur Cloud oder zu Drittanbietern).

Die **Industrie** in der Grafik wirkt verhältnismäßig „technisch konservativ“. Dies wird durch weniger Impact, weniger Exfiltration, mehr Fokus auf Zugang, Ausführung und Bewegung reflektiert. Industrieunternehmen haben oft komplexe heterogene IT/OT-Umgebungen, nutzen Detektionsmöglichkeiten aber häufig flächendeckend und pragmatisch aus operativer Notwendigkeit. Von einigen spezialisierteren Industrien abgesehen, liegt die Motivation der Angreifer im Kontext Industrie häufig im Bereich Cybercrime bzw. Ransomware. Die genutzten und detektierten Techniken stützen diese These.

In der Industrie sind Execution, Lateral Movement und Credential Access auffällig. Das zeigt, dass Angreifer nach dem Erstzugang versuchen, Produktions- oder Unternehmensnetze weiter zu durchdringen.

Sektor	Hauptrisiken	Empfohlene Maßnahmen
Öffentlicher Sektor	Persistence, Command & Control, Discovery	Threat Hunting & Monitoring, EDR/XDR, Zero-Trust, Segmentierung
Industrie	Execution, Lateral Movement, Credential Access	IT-/OT-Trennung, IAM stärken, EDR/XDR, Supply-Chain-Absicherung
Einzelhandel	Exfiltration, Impact, Payment-System-Angriffe	Datenverschlüsselung, EDR/XDR, Red-Teaming
IT & Finanzen	Credential Access, Command & Control, Exfiltration	MFA verpflichtend, EDR/XDR & KI-Analyse, Datenflusskontrollen

Abbildung 3: Übersicht der Empfehlungen nach Sektoren

Empfehlungen:

- **Trennung von IT- und OT-Netzen** konsequent durchsetzen, um eine Ausbreitung zu verhindern.
- Starke **Identity & Access Management (IAM)**-Kontrollen, um Credential-Diebstahl zu erschweren.
- **Dediziertes Monitoring von Anomalien in der Produktions-IT (ICS/SCADA)**, mindestens im „IT-Teil“ der OT.
- Vorbereitung auf **Supply-Chain-Angriffe**, z. B. über Dienstleister oder Software-Lieferanten.

Der **Einzelhandel** zeigt einen relativen Anteil an Impact und Exfiltration, mehr als manche Industriebetriebe. Das ergibt Sinn, weil Angriffe gegen Kundendaten, Zahlungssysteme oder Geschäftsgeheimnisse im Handel schnell monetär relevant werden.

Empfehlungen:

- **Datenverschlüsselung und -maskierung** bei Kunden- und Zahlungsinformationen.
- Starke **Absicherung von POS-Systemen und Payment-Gateways** gegen Malware und Phishing.

- Regelmäßige **Red-Teaming-Übungen**, um den Umgang mit Vorfällen mit potenziell direktem Geschäftsschaden zu trainieren.

Schlussfolgerung aus unserer Analyse

Wir sehen, dass die Angriffstaktiken sehr klar entlang einer typischen Kill-Chain verlaufen: Nach Reconnaissance kommt Initial Access, dann Execution, Credential/Privilege Escalation, Discovery, Lateral Movement, schließlich Exfiltration oder Impact. Je nach Branche ändern sich die Schwerpunkte.

Diese Erkenntnisse verdeutlichen, in welchen Bereichen Organisationen ihre Abwehr besonders stärken müssen:

- Zwingender Einsatz von EDR/XDR-Systemen zur granularen Analyse von hochwertigen Telemetriedaten. Dies ist Voraussetzung dafür, Angriffe präzise, unter Berücksichtigung der Angreifertools und -techniken zu analysieren und einen Angriff direkt in der Entstehung abzuwehren.
- Netzwerksegmentierung und Monitoring, um laterale Bewegung zu begrenzen.

Projektion für die nächste Periode

Wir erwarten, dass Lateral Movement und Discovery branchenübergreifend noch wichtiger werden, da Angreifer verstärkt versuchen, unentdeckt tief in Netzwerke vorzudringen.

Credential Access wird durch gestohlene Identitäten und den Missbrauch von Cloud-Diensten weiter zunehmen.

Exfiltration und Impact werden sich im Einzelhandel und Finanzwesen verstärken, da die Monetarisierung von Daten im Vordergrund steht.

Für die **Industrie** sehen wir ein steigendes Risiko für schwerwiegendere OT-Angriffe, insbesondere durch geopolitische Spannungen und staatlich unterstützte Gruppen.



4. Analyst Spotlight

ClickFix – Social Engineering-Technik

ClickFix ist eine Phishing-Taktik, die Benutzer gezielt täuscht und sie dazu bringt, eigenständig schädlichen Code auszuführen. Sie wurde Anfang 2024 zum ersten Mal von Proofpoint berichtet. Seit ihrer Entdeckung wird sie von verschiedenen Angreifern verwendet. Seit Anfang 2024 ist ihre Nutzung sehr schnell angestiegen.

Der Hauptgrund für die schnelle Verbreitung ist, dass sie Benutzer leicht täuschen kann und keine komplexen Infrastrukturen benötigt. Die natürliche Problemlösungsneigung von Anwendern führt oft dazu, dass sie Fehler machen – etwa schädlichen Code ausführen oder Malware herunterladen. Verschiedene Angreifergruppen nutzten diese Taktik, um sehr unterschiedliche Malware zu verbreiten. Die am häufigsten verbreiteten Malware-Familien sind Lumma Stealer, DarkGate, Vidar Stealer, SnakeStealer, Stealc, Rhadamanthys, Latrodectus, MintsLoader, Xworm, AsyncRAT, NetSupport, SectopRAT.

In einem typischen ClickFix-Szenario wird das Opfer auf eine Webseite mit einer falschen Fehlermeldung oder Warnung weitergeleitet. Diese Warnungen behaupten meist, dass

die Seite oder das Dokument nicht richtig angezeigt werden kann, und fordern zum Klicken auf einen „Verify“ oder ähnliche Button auf, um das Problem zu lösen. Wenn dieser Button geklickt wird, kopiert ein schädliches JavaScript im Hintergrund unbemerkt einen Befehl in die Zwischenablage des Opfers. Danach wird der Benutzer aufgefordert, die Win+R-Tastenkombination zu verwenden, um das Ausführen-Fenster zu öffnen, den Code aus der Zwischenablage mit Ctrl+V einzufügen und durch Drücken der Enter-Taste auszuführen. Diese Phase ist der kritischste Punkt des Angriffs, denn der schädliche Code wird nur durch die direkte Handlung des Benutzers ausgeführt. Dies unterscheidet ClickFix von klassischen Malware-Download-Methoden und ermöglicht es, Browser-Sicherheitsmaßnahmen wie Smart Screen und Google Safe Browsing zu umgehen.

Maßnahmen

Es können Gruppenrichtlinien im Active Directory implementiert werden, die verhindern, dass eingebaute Windows-Programme wie powershell.exe über das Ausführen-Dialogfeld gestartet werden; jedoch sollte nicht vergessen werden, dass Angreifer versuchen können, dies mit manuellen Anweisungen zu

umgehen. Technische Maßnahmen sind allein gegen Angriffe, die das Vertrauen und Verhalten der Benutzer ausnutzen, nicht ausreichend. Organisationen sollten ihre Mitarbeiter mit kontinuierlichen und zielgerichteten Awareness-Schulungen sensibilisieren.

Grundlegende Punkte, die die Awareness-Schulungen abdecken sollten:

- Unerwartete Pop-ups und falsche Fehlermeldungen unterscheiden
- Wissen, dass legitime Dienste niemals verlangen würden, Code in die Systembefehlszeile zu kopieren und einzufügen
- Sich der Risiken bei der Verwendung von Win+R und Ctrl+V bewusst sein, besonders wenn man von unsicheren Quellen weitergeleitet wird

AiTM (Adversary in the middle) Attack

AiTM-Phishing-Angriffe bilden seit einiger Zeit die Speerspitze der identitätsbasierten Initial-Access-Methoden. Die großflächige Einführung von Multifaktor-Authentifizierungen hat die Angreifer gezwungen, von klassischen Passwort-basierten-Phishing

Neue ClickFix-Varianten: Win+X und FileFix

Angreifer entwickeln ihre Techniken ständig weiter und haben auch bei ClickFix weitere neue Varianten entwickelt, die darauf abzielen, Beschränkungen zu umgehen, die Benutzer daran hindern, Schadcode auszuführen bzw. die Erkennung des Angriffs zu erschweren.

Windows Power User Menü (Win+X): In dieser Variante wird der Benutzer angewiesen, die Win+X-Tastenkombination zu drü-

cken und dann ein Terminal (zum Beispiel PowerShell) zu öffnen. Der Benutzer fügt den schädlichen Befehl, der zuvor in seine Zwischenablage kopiert wurde, in dieses Terminal ein und führt ihn aus.

FileFix: Nutzt die Tatsache aus, dass die Adressleiste des Windows File Explorers Betriebssystembefehle ausführen kann, und Browser dieses Verhalten nicht blockieren.

Ein FileFix-Angriff umfasst normalerweise folgende Schritte:

- Das Opfer wird dazu verleitet, auf einen Button wie „Start

Verification“ auf einer gefälschten CAPTCHA- oder Verifizierungsseite zu klicken. Dieser Vorgang öffnet den Windows File Explorer.

- Die Seite fordert den Benutzer auf, die Tastenkombination Ctrl + L zu verwenden, um die Adressleiste auszuwählen.
- Danach wird der Benutzer aufgefordert, den schädlichen Befehl, der in seine Zwischenablage kopiert wurde, mit Ctrl + V einzufügen und die Enter-Taste zu drücken.

Angriffen auf eine neuartige Methode umzusteigen, die den zweiten Faktor umgeht.

Optisch ist AiTM oft nicht vom herkömmlichen Credential Phishing zu unterscheiden; der entscheidende Unterschied liegt jedoch in der Automatisierung des MFA requests und der Nutzung eines Reverse Proxies, um alle Benutzerinteraktionen auf die Systeme des Angreifers umzuleiten. Die Angreifer nutzen hierzu bestimmte Tools (EvilGinx, Modlishka, Muerena), um diese Angriffe weitgehend automatisiert und mit minimalem Aufwand durchzuführen.

Der Benutzer wird wie beim klassischen Credential Phishing auf eine Anmeldeseite weitergeleitet. Gibt der Benutzer hier seine Zugangsdaten ein, leitet der Reverse Proxy die Anmeldeanfrage direkt an die offizielle Seite weiter und reicht dem Benutzer sogar den MFA-Prompt weiter. Für den Benutzer stellt die Anmelde- maske und das Verhalten der Seite keine offensichtliche Abnormalität dar – was es dem Benutzer erschwert den Angriff von einer legitimen Anmeldung zu unterscheiden. Wenn der Benutzer den MFA-Prompt bestätigt, leitet der Angreifer den Prompt an die Anmeldeseite weiter und vollendet die Anmeldung. Durch die erfolgreiche Anmeldung wird ein sogenanntes Session Cookie erstellt.

Das eigentliche Ziel des Angreifers ist dabei das Session-Cookie. In diesem Cookie ist vermerkt, dass sich der Benutzer erfolgreich angemeldet und seine Identität per MFA bestätigt hat. Der Angreifer kann dieses Cookie nun nutzen, um sich direkt im Kontext des Benutzers anzumelden. Es ist keine weitere Authentifizierung erforderlich.

Was auf die Kompromittierung folgt, ist oft unterschiedlich, aber die am häufigsten beobachtete Methode für Persistenz ist das Einpflegen eines eigenen zweiten Faktors. Der Angreifer hat durch das Phishing bereits die Zugangsdaten des Benutzers und durch das Hinzufügen eines eigenen zweiten Faktors kann der Angreifer sich jederzeit erneut anmelden, selbst wenn der Session Cookie ausläuft.

Wie erkenne ich einen AiTM-Angriff?

AiTM-Angriffe sind oft tückisch aber können mit den entsprechenden Security Tools oder SIEM Use Cases aufgedeckt werden.

XDR-Systeme wie Microsoft Defender haben eingebaute Erkennungsregeln, um das oben beschriebene Verhalten zu erkennen und können den Benutzer automatisch sperren, um so weiteren Schaden zu verhin-

dern. Allgemeine Phishing-Alarme können auch durch adäquate Nachqualifizierung auf einen AiTM-Angriff hinweisen.

Wie kann ich mich dagegen schützen?

Die effektivste Methode, um AiTM-Angriffe abzuwehren, ist eine konsequente Implementierung von Conditional Access Policies. Die Anmeldungen des Angreifers erfolgen von einem unbekannten Gerät und genau hier bietet eine Conditional Access Policy Möglichkeiten zur Erkennung und Abwehr der Angriffe.

Eine Conditional Access Policy, die eine Anmeldung nur zulässt, wenn das Gerät im Tenant bekannt ist (Hybrid-Joined) verhindert, dass der Angreifer sich mit seinem gestohlenen Cookie anmelden kann.

Prävention oder Minderung des Schadens sind durch folgende Maßnahmen möglich:

- Integrierte Alarmierung: Microsoft 365 Defender/ Azure AD Identity Protection
- Phishing-resistente MFA-Lösungen

Die **Controlware GmbH** zählt zu den Markt- und Qualitätsführern unter den IT-Dienstleistern und Managed Service Providern in Deutschland. Das Unternehmen ist Teil der Controlware Gruppe mit insgesamt rund 1.000 Mitarbeitenden und einem Umsatz von über 500 Mio. Euro, zu der auch die Networkers AG sowie Controlware Österreich gehören.

Als Digitalisierungspartner von mittelständischen und großen Unternehmen sowie von Behörden und Einrichtungen der öffentlichen Hand entwickelt, implementiert und betreibt Controlware agile und resiliente IT-Lösungen in den Bereichen **Network Solutions, Information Security, Data Center & Cloud,**

Collaboration, IT-Management und Managed Services – und unterstützt Kunden dabei, die Weichen für einen wirtschaftlichen, zukunfts-sicheren und nachhaltigen IT-Betrieb zu stellen. Dabei stehen wir unseren Kunden in allen Projektphasen zur Seite: von der Beratung und Planung bis hin zur Realisierung und Wartung.

Als MSP mit einem eigenen **ISO 27001-zertifizierten Customer Service Center** reicht unser Angebot von Betriebsunterstützung bis zu kompletten Managed Services für Cloud-, Data Center-, Enterprise- und Campus-Umgebungen. Zudem bieten wir umfassende **Cyber Defense Services**. Neben unserem eigenen flächendeckenden Vertriebs- und

Servicenetzt mit **14 Standorten in DACH**, die gemäß ISO 9001-zertifiziert sind, unterhalten wir internationale Partnerschaften und sind so in der Lage, anspruchsvolle globale Projekte abzuwickeln.

Seit unserer Gründung im Jahr 1980 arbeiten wir eng mit den nationalen und international führenden Herstellern sowie innovativen Newcomern zusammen und sind bei den meisten dieser Partner im höchsten Qualifizierungsgrad zertifiziert. Besonderes Augenmerk legen wir auf die Nachwuchsförderung: Seit vielen Jahren kooperieren wir mit renommierten deutschen Hochschulen und betreuen durchgehend rund 50 Auszubildende und Studenten.

- FIDO / zertifikatsbasierte Authentifizierung und keine SMS / Anruf
- Schutz vor Angriffen durch Conditional Access Policy
 - Hybrid Joined
 - Compliance Based
- Kurze Haltbarkeit von Session Tokens
- Dedizierte Alarmüberwachung (internes oder externes SOC)

Direkter Kontakt gewünscht?

Unser Expertenteam steht Ihnen für Fragen zur Verfügung!

✉ threatreport@controlware.de

Unsere Standorte

Deutschland

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach

Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf:



Berlin

Tel. +49 30 67097-0
info-ber@controlware.de

Düsseldorf

Tel. +49 2159 9696-0
info-due@controlware.de

Frankfurt/Main

Tel. +49 6074 858-206
info-ffm@controlware.de

Hagen

Tel. +49 2331 8095-0
info@networkers.de

Hamburg

Tel. +49 40 251746-0
info-ham@controlware.de

Hannover

Tel. +49 511 726092-0
info-han@controlware.de

Ingolstadt

Tel. +49 841 23222-0
info-ing@controlware.de

Kassel

Tel. +49 561 47576-0
info-kas@controlware.de

Leipzig

Tel. +49 341 98387-30
info-lei@controlware.de

München

Tel. +49 89 666367-0
info-muc@controlware.de

Stuttgart

Tel. +49 711 770568-0
info-stu@controlware.de

Wolfsburg

Tel.: +49 5362 9993413
info-wey@controlware.de

Österreich

Innsbruck

Tel. +43 512 345200
info@controlware.at

Wien

Tel. +43 1 890 0724-0
info@controlware.at