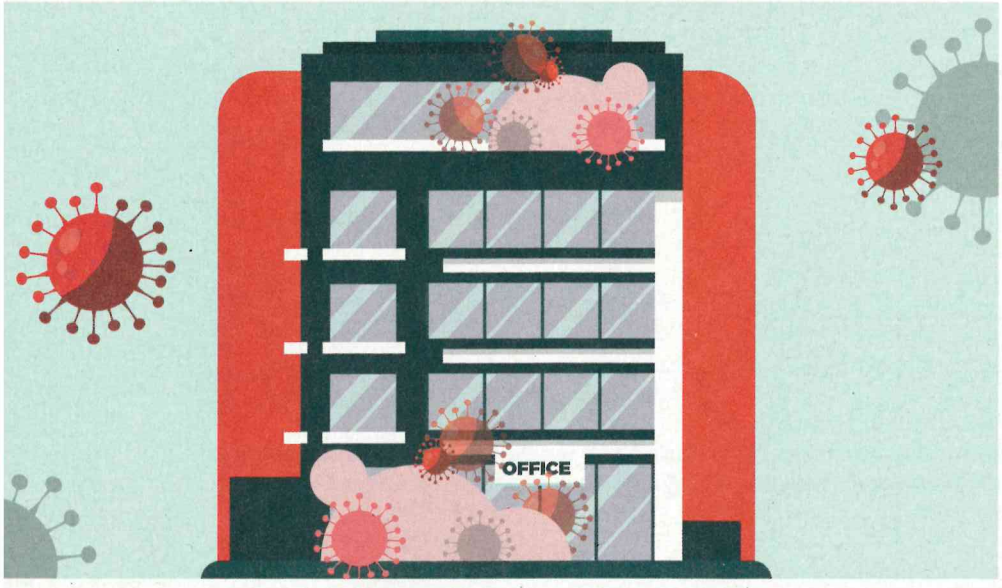


Was tut sich bei der Sicherheit?

IT-Security erfordert eine ständige Überprüfung und Weiterentwicklung von Sicherheitsmaßnahmen. Wie ist der Stand der Dinge bei Malware und Co. und was verändert sich durch SOC-Architekturen und künstliche Intelligenz? Eine Analyse im Unternehmenskontext.

Von Stefan Strobel

Neue Entwicklungen in der IT führen fast immer auch zu neuen Schwachstellen. Schnell nutzen Kriminelle sie aus, um ihre Opfer zu betrügen oder um in Unternehmensnetze einzudringen. Durch die neuen Entwicklungen entstehen aber meist auch neue Sicherheitstechniken, mit denen man sich vor Angriffen schützen kann. Die Einführung von Smartphones, der Trend zu Cloud-Services oder die neuen technischen Möglichkeiten durch künstliche Intelligenz zeigen dies deutlich. Aber auch unabhängig von technischen Neuerungen kann man einen Wettlauf zwischen Angreifern und Verteidigern beobachten.

Schon lange im Fokus: Authentisierung

Ein offensichtliches Beispiel ist die Authentisierung. Nachdem vor langer Zeit Passwörter eingeführt wurden, um unbefugten Zugriff auf IT-Systeme zu verhindern, wurden ihre Schwächen schnell ausgenutzt und Angreifer haben Passwörter mit Brute-Force-Angriffen erraten. Erste Maßnahmen wie temporäres Sperren nach mehreren Fehlversuchen hebelten sie mit Password Spraying oder Phishing aus. Noch vor wenigen Jahren galt dann eine Zwei-Faktor-Authentisierung (2FA) als die Lösung schlechthin. Mittlerweile haben wohl fast alle Unternehmen ihre externen Zugänge mit 2FA-Token oder entsprechenden Apps auf Smartphones abgesichert. Das wiederum hat die Angreifer motiviert nachzurüsten: Sie griffen beim Phishing per „Adversary in the Middle" an, das gängige 2FA-Methoden umgehen kann. Als Konsequenz sind Unternehmen gezwungen, ihre Anmeldungen auf phishingresistente Methoden wie Passkeys oder FIDO-Keys umzustellen.

Da sich also die Angriffe ständig weiterentwickeln, ändert sich die Bedrohungslage permanent und damit auch die Wirksamkeit der umgesetzten Sicherheitsmaßnahmen. Aber auch die Gesetzgebung trägt ihren Teil zur permanenten Änderung in der Securitybranche bei. Ständig neue Complianceframeworks und Vorgaben erfordern ebenfalls Änderungen sowohl in der Technik als auch in der Organisation der Informationssicherheit.

Es ist daher unabdingbar, sich ständig mit den Änderungen zu beschäftigen, neue Trends und Buzzwords im Auge zu behalten und aus der geänderten Bedrohungslage, der oft reduzierten Wirksamkeit gerade erst eingeführter neuer Maßnahmen und Vorschriften den Handlungsbedarf für die eigene Organisation abzuleiten. Dieser Artikel greift einige der aktuellen Entwicklungen auf und ordnet sie in den Kontext eines Unternehmens ein.

Aktuelle Entwicklungen bei Ransomware

Betrachtet man die derzeit auffälligsten Angreifer – Kriminelle, die Unternehmen ihre Daten stehlen und verschlüsseln, um dann Lösegeld zu erpressen –, so sind auch diese Ransomware-Akteure in einem ständigen Wandel. Die einzelnen Gruppierungen, die sich seit Jahren auf Teilaspekte des kriminellen Ökosystems fokussiert haben, formieren sich ständig neu, werden von international zusammenarbeitenden Polizeibehörden zerschlagen, von rivalisierenden Gruppierungen gehackt oder verschwinden von

iX-TRACT

- Neue Entwicklungen in der IT gehen oft mit neuen Bedrohungstrends einher und ziehen neue Klassen von Sicherungstechniken und Schutzprodukten nach sich.
- Die mittlere Zeit zwischen der Veröffentlichung eines Patches und der Ausnutzung der damit behobenen Schwachstelle ist auf fünf Tage gesunken.
- Viele Schwachstellen werden zudem meist schon als Zero Days für Angriffe genutzt.
- Der erste Schritt zu mehr Sicherheit ist, sich kontinuierlich über Trends und neue Entwicklungen zu informieren und diese im eigenen Organisationskontext zu bewerten.

der Bildfläche. Die technischen Schwerpunkte der Einbrüche verschieben sich ständig und neue Tricks zur Täuschung der Opfer werden bekannt und setzen sich durch.

So sieht man in den letzten Jahren eine immer stärkere und frühzeitigere Ausnutzung von Softwareschwachstellen durch die Angreifer. In den Statistiken zu den am häufigsten ausgenutzten Schwachstellen der letzten zwei Jahre liegen Firewall- und VPN-Produkte oder Produkte für sicheren Dateiaustausch ganz vorn. Die Tabelle „Die 2023 am häufigsten ausgenutzten Schwachstellen" zeigt exemplarisch die Daten für 2023. Aus Sicherheitsprodukten werden also Einstiegspunkte für Kriminelle.

Die Ransomwaregruppe Clop beispielsweise hat sich seit Jahren darauf spezialisiert, Schwachstellen in kommerziellen Produkten für den sicheren Austausch von Dokumenten zu suchen und diese dann massenhaft auszunutzen, um die vertraulichen Daten ihrer Opfer zu stehlen und diese mit einer Veröffentlichung zu erpressen. Im Jahr 2023 traf es Tausende Kunden der Datenübertragungssoftware MOVEit und 2025 die Anwender von Cleo aus derselben Produktkategorie. Aber auch die Kunden von Fortinet, Ivanti oder Palo Alto waren in den letzten Monaten immer wieder gezwungen, kurzfristig Patches zur Behebung kritischer Sicherheitslücken in ihren Firewalls oder VPN-Produkten einzuspielen.

Das Erschreckende dabei ist, wie schnell die Angreifer bei solche Sicherheitslücken inzwischen sind. Schon im Jahr 2023 haben sie die meisten dieser Schwachstellen als Zero Days ausgenutzt. Die betroffenen Kunden konnten also noch gar nicht wissen, dass es eine so kritische Schwachstelle in ihrem Sicherheitsgateway gab, und einen Patch gab es natürlich auch noch nicht. Die mittlere Zeit zwischen der Veröffentlichung eines Patches und der Ausnutzung durch Angreifer ist nach einer Statistik von Mandiant auf fünf Tage gesunken (siehe ix.de/zf4s). Wer bisher extern erreichbare Systeme mit einer Verzögerung von einer Woche oder mehr gepatcht hat, muss nun offensichtlich seine Prozesse überdenken.

Phishing und Malware: immer noch akut

Der Trend zur Ausnutzung von Schwachstellen bedeutet jedoch nicht, dass Phishing oder Malwareinfektionen beim Websurfen bedeutungslos geworden wären. In Statistiken zur Erstinfektion mit Malware hat SocGholish in den letzten zwölf Monaten mit Abstand Platz eins belegt (siehe Abbildung 1 und 2). Diese Malware wurde bevorzugt über vorgetäuschte Software-Updates verteilt. Benutzer bekommen beim Besuch entsprechend manipulierter Websites den Hinweis, dass der Browser veraltet sei, und einen Link, um ihn schnell zu aktualisieren. Wer das vermeintliche Update über diesen Link installiert, infiziert sein System mit SocGholish, das dann eine Hintertür platziert und den Zugang dazu auf den einschlägigen Darknet-Marktplätzen weiterverkauft (siehe ix.de/zf4s). Aber auch Stealer wie Lumma, RedLine und ständig neue Varianten haben in den letzten Monaten Zugangsdaten auf den Endgeräten betroffener Benutzer ausspioniert, um Angreifern weiteren Zugriff auf die Systeme des Opfers zu ermöglichen.

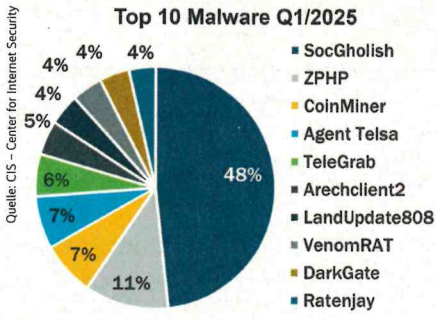
Neben dem klassischen Phishing per E-Mail sieht man in den letzten Monaten oder sogar Jahren Trends zu neuen Varianten wie Vishing [1] oder Callback-Phishing. Bei Vishing ruft ein Angreifer seine Opfer an, oft mit gefälschter Anrufertelefonnummer, und überzeugt sie, manipulierte Webseiten zu besuchen, sich dort anzumelden, Schadsoftware auszuführen oder eine Hintertüre zu öffnen. Mithilfe spezieller Proxys wie Evilginx oder Modlishka kann der Angreifer dann beispielsweise die Anmeldung seines Opfers an M365 nutzen, auch wenn die Authentisierung über einen zweiten Faktor vermeintlich abgesichert, aber nicht phishingresistent war.

Beim Callback-Phishing wird noch eine klassische E-Mail verwendet, die aber weder einen Link noch ein potenziell verseuchtes Attachment enthält. Die E-Mail könnte beispielsweise eine Zahlungsaufforderung enthalten. Ein Opfer, das sich keiner Bestellung bewusst ist, wird so dazu verleitet, die zusammen mit der Adresse des vorgetäuschten Verkäufers angegebene Telefonnummer anzurufen. Dort übernimmt dann ein Callcenter alles Weitere und überzeugt das Opfer, Webseiten zu besuchen und letztlich Schadsoftware auszuführen. Der Kasten „An-

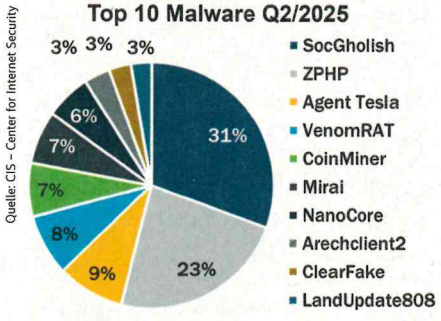
Quelle: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a

Die 2023 am häufigsten ausgenutzten Schwachstellen

CVE	Anbieter	Produkt(e)	Schwachstellentyp
CVE-2023-3519	Citrix	NetScaler ADC NetScaler Gateway	Code Injection
CVE-2023-4966	Citrix	NetScaler ADC NetScaler Gateway	Buffer Overflow
CVE-2023-20198	Cisco	IOS XE Web UI	Privilege Escalation
CVE-2023-20273	Cisco	IOS XE	Web UI Command Injection
CVE-2023-27997	Fortinet	FortiOS FortiProxy SSL-VPN	Heap-based Buffer Overflow
CVE-2023-34362	Progress	MOVEit Transfer	SQL Injection
CVE-2023-22515	Atlassian	Confluence Data Center and Server	Broken Access Control
CVE-2021-44228	Apache	Log4j2	Remote Code Execution (RCE)
CVE-2023-2868	Barracuda Networks	ESG Appliance	Improper Input Validation
CVE-2022-47966	Zoho	ManageEngine Multiple Products	Remote Code Execution
CVE-2023-27350	PaperCut	MF/NG	Improper Access Control
CVE-2020-1472	Microsoft	Netlogon	Privilege Escalation
CVE-2023-42793	JetBrains	TeamCity	Authentication Bypass
CVE-2023-23397	Microsoft	Office Outlook	Privilege Escalation
CVE-2023-49103	ownCloud	graphapi	Information Disclosure



Die Malware SocGholish dominierte im ersten Quartal die vom CIS herausgegebene Malware-Top-10-Liste (Abb. 1).



Trotz großer Dynamik bei den beteiligten Schädlingen blieb SocGholish auch im zweiten Quartal 2025 die häufigste Malwarevariante (Abb. 2).

griffsvektoren von Top-10-Malware“ gibt einen Überblick der Dynamik der letzten zwei Jahre.

Lieferketten stärker im Fokus

Angriffe über die Softwarelieferkette sind ein weiterer Trend, der zwar nicht neu ist, aber immer relevanter wird. Oft sind große Unternehmen so gut geschützt, dass ein Angreifer über einen Lieferanten seines finalen Opfers einfacher ans Ziel kommt. Kleinere und schlechter gesicherte IT-Dienstleister, die Remote-Zugriff auf die IT ihrer Kunden haben, sind offensichtliche Einfallstore. Als Folge stellen große Unternehmen schon lange immer höhere Anforderungen an die Sicherheit ihrer Lieferanten. Lieferketten sind aber, wie der Name schon suggeriert, keine kurzen Verbindungen, sondern oft länger. Ein IT-Dienstleister implementiert beispielsweise bei seinem Kunden ein IT-Produkt, das der Dienstleister nicht selbst entwickelt hat, sondern von einem Hersteller einkauft und an den Endkunden weiterverkauft. Der Hersteller wiederum hat das Produkt auch nicht vollständig selbst entwickelt, sondern verwendet Komponenten eines weiteren Herstellers. Und dieser Hersteller setzt in seiner Komponente auf Open-Source-Bibliotheken, die gegebenenfalls andere, kleinere Bibliotheken nutzen.

Jeden Monat findet man zahlreiche neu mit Schadsoftware verseuchte Bibliotheken oder Komponenten in der Advisory-Liste von GitHub. Viele davon haben keinen anderen Zweck, als mit ihrer vermeintlichen Nützlichkeit zu werben und so Hintertüren in die Produkte von Softwareherstellern einzuschleusen. Ein dramatisches Beispiel war die Hintertür in den XZ-Utils, einem kleinen, unscheinbaren Open-Source-Projekt für Datenkompression. Ein Angreifer hat es durch jahrelange Bemühungen geschafft, sich mit mehreren vorgetäuschten Identitäten als vertrauenswürdiger Mitentwickler in diesem Projekt zu positionieren, um dann eine gut versteckte Backdoor einzubauen. Wenn diese nicht beinahe zufällig entdeckt worden wäre, dann könnte der Angreifer sie möglicherweise heute dazu verwenden, eine große Zahl Linux-basierter Systeme im Internet heimlich zu kontrollieren.

Der Trend zu Angriffen über die Lieferkette und insbesondere über Softwarekomponenten und eingebundene Bibliotheken führt auch zu einem Trend aufseiten der Schutzmaßnahmen. Werkzeuge zur Software Composition Analysis (SCA) oder noch weiter gehende für Application Security Posture Management (ASPM [2]) bringen schon während der Entwicklung Informationen zu den genutzten Komponenten und den in der nächsten Ebene verwendeten Bibliotheken ein. Sie erzeugen Stücklisten für die Bestandteile der Software – Software Bills of Materials (SBOM). ASPM-Produkte ergänzen dann Informationen über Schwachstellen aus verschiedenen Prüfwerkzeugen und Quellen, korrelieren die Informationen miteinander, um nicht nur die bei der eigenen Entwicklung entstandenen Schwachstellen zu entdecken, sondern auch die aus fremden Komponenten stammenden im Kontext zu bewerten.

Neue Gefahren durch KI

Künstliche Intelligenz spielt im Gesamtbild bei Angriffen noch keine große Rolle, ist aber ein spannender neuer Trend, denn mit LLMs können Angreifer schnell und ohne eigene Sprachkenntnisse Phishingtexte in allen denkbaren Landessprachen erzeugen. Deepfakes täuschen Sprachnachrichten oder sogar Anrufe mit der Stimme eines Kollegen oder Chefs vor. Selbst gefälschte Videoanrufe sind technisch schon machbar und dürften in Zukunft verstärkt von Angreifern genutzt werden.

Künstliche Intelligenz ist aber nicht nur im Kontext von Phishing und Deepfakes eine neue Bedrohung. Auch die Nutzung von KI-Systemen wie ChatGPT, Copilot und anderen durch Mitarbeiter eines Unternehmens erzeugt neue Gefahren. Wer mal eben einen deutschen Text zur Übersetzung ins Französische in die Website einer KI im Internet kopiert, gibt damit möglicherweise vertrauliche Inhalte

Angriffsvektoren von Top-10-Malware

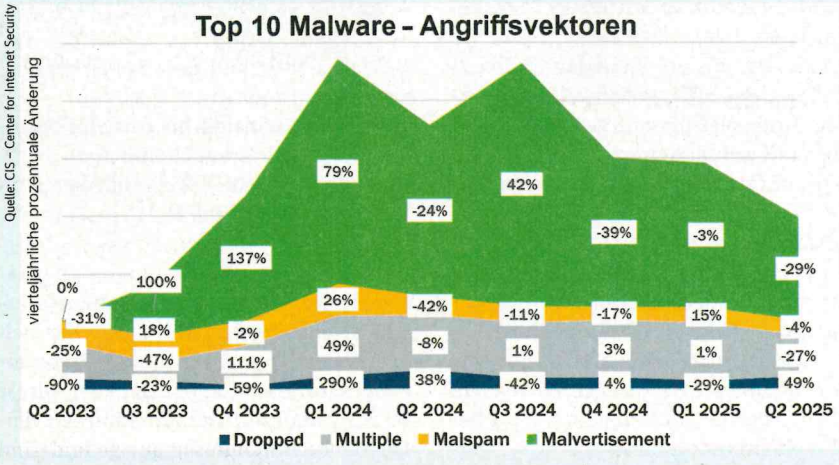
Die initialen Angriffsvektoren für Malware lassen sich laut CIS für die Top 10 im zweiten Quartal 2025 in vier Kategorien einsortieren (siehe ix.de/zf4s).

Dropped: Malware, die von anderer Malware, die sich schon auf dem System befindet, etwa einem Exploit-Kit oder einer infizierten Drittanbietersoftware, automatisch bereitgestellt oder manuell von einem Cyberangreifer nachgeladen wird. Mirai ist die Bedrohung auf der CIS-Top-10-Malware-Liste für Q2/2025, die diese Technik zum Zeitpunkt der Top-10-Veröffentlichung nutzt.

Malspam: Unerwünschte E-Mails, die Benutzer entweder auf bösartige Websites leiten oder sie dazu verleiten, Malware herunterzuladen oder zu öffnen. Derzeit setzt von den Top 10 Agent Tesla diese Technik ein.

Malvertisement: Über bösartige Werbeanzeigen eingeschleuste Malware. Von der Top-10-Liste verwenden ClearFake, LandUpdate808, SocGholish und ZPHP diese Technik.

Multiple klassifiziert Malware, die mindestens zwei Vektoren verwendet, etwa Dropped und Malspam. In den Top 10 gehören ArechClient2, CoinMiner, NanoCore und VenomRat dazu.



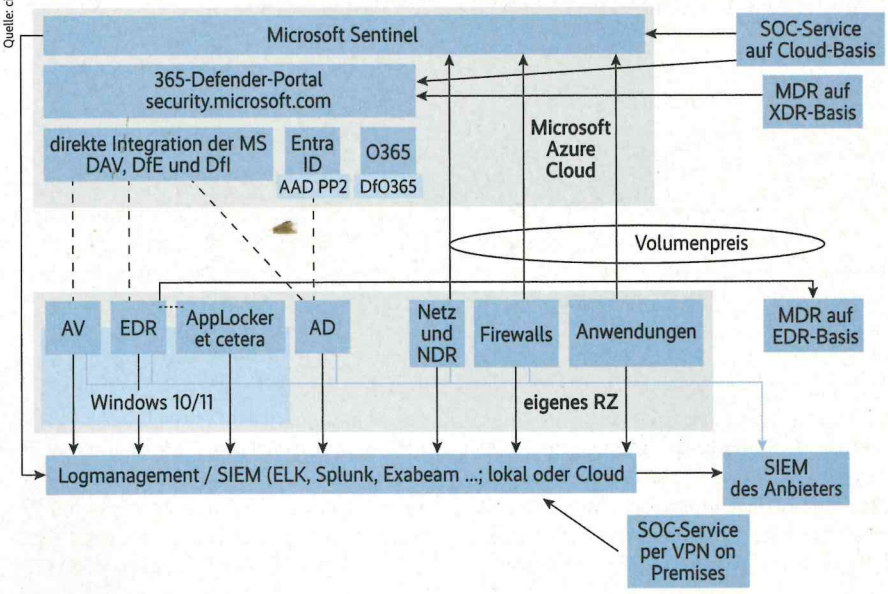
Im Gegensatz zur großen Dynamik bei Angriffen per Malvertisement ändert sich bei den komplexeren kombinierten Methoden deutlich weniger an der groben Verteilung (Abb. 3).

in die Hände des KI-Betreibers. Gleiches gilt für Entwickler, die in ihrer Umgebung ein KI-Plug-in verwenden. Da der gerade im Editor geöffnete Quellcode von der KI vervollständigt werden soll, wird er auch im Hintergrund an den Cloud-Service der KI im Internet gesendet – und mit ihm eventuell enthaltene Credentials, Access-Token oder API-Keys.

Auch wenn man für Kunden oder Mitarbeiter eigene KI-Systeme bereitstellt und diese mit internen Dokumenten trainiert, ergeben sich daraus neue Risiken, denn möglicherweise hat die KI auch vertrauliche Details gelernt und kann diese bei geschickt formulierten Anfragen wieder preisgeben, wie die Artikel „Angriffe auf große Sprachmodelle“ [3] und „Agentic AI aus Securitysicht“ [4] ausführlich beschreiben. Die Beschränkungen, die man der KI bei der Erstellung mitgegeben hat, werden von immer neuen Tricks ausgehebelt.

SOC-/MDR-Architekturen – klassischer Ansatz Managed SOC

Quelle: cirosec



Art und Ebene der Integration eines SOC-Service mit der Infrastruktur der Kunden hat große Auswirkungen auf die Erkennungsfähigkeit und die Kosten (Abb. 4).

Neue Securitytools durch KI

Die KI erzeugt jedoch nicht nur neue Bedrohungen, sondern generiert auch einen Markt für neue Sicherheitsprodukte. Einerseits zum Schutz vor KI-basierten Angriffen wie Deepfakes – hier kommen wieder KI-Modelle zum Einsatz, um Deepfakes während eines Telefonats oder einer Videokonferenz zu erkennen –, andererseits um die neuen Risiken durch legitime Nutzung von KI zu verringern. Letzteres sind Produkte zum Schutz der eigenen KI-basierten Services beziehungsweise Chatbots oder aber Produkte zum Erkennen und Verhindern von Datenabfluss bei der Nutzung von KIs im Internet. Diese Tools erkennen zum Beispiel, wenn ein Quelltext API-Keys enthält. Diese Keys werden dann auf dem Weg zur KI durch Platzhalter ersetzt.

Auch unabhängig von den Risiken, die erst durch KI entstehen, gibt es neue Produkte auf Basis von KI, die Unternehmen sicherer machen sollen oder den Mitarbeitern in der Sicherheitsabteilung oder im Security Operations Center (SOC) bei der täglichen Arbeit helfen. Virtuelle SOC-Mitarbeiter, die eigenständig Alarme bearbeiten, Daten anreichern und Zusammenfassungen schreiben, oder die schon länger etablierten Produkte zur Klassifikation von Schadsoftware mit neuronalen Netzen oder zur Erkennung von Anomalien im Datenverkehr sind gute Beispiele dafür.

In vielen Bereichen der IT-Sicherheit testen die Hersteller neue Features ihrer Produkte auf Basis von LLMs, die die Kommunikation mit dem Produkt in natürlicher Sprache ermöglichen. Regeln, Prozesse oder Automatisierungsabläufe sollen so auf Englisch beschrieben und von der KI-Erweiterung im jeweiligen Produkt konfiguriert werden. Genauso lassen sich Meldungen oder insbesondere Alarme von einem KI-Modul mit Kontext anreichern und dem Empfänger in normalem englischen Text erläutern.

Anstatt Automatisierungen wie früher in einem SOAR-Werkzeug grafisch Schritt für Schritt aus Bausteinen zusammenzuklicken, kann man einigen Produkten in englischem Text beschreiben, was man automatisieren möchte, und das LLM erzeugt daraus die Grundkonfiguration. Eine Unterstützung für andere Sprachen wie Deutsch ist oft geplant, aber in den meisten Fällen bisher noch nicht implementiert.

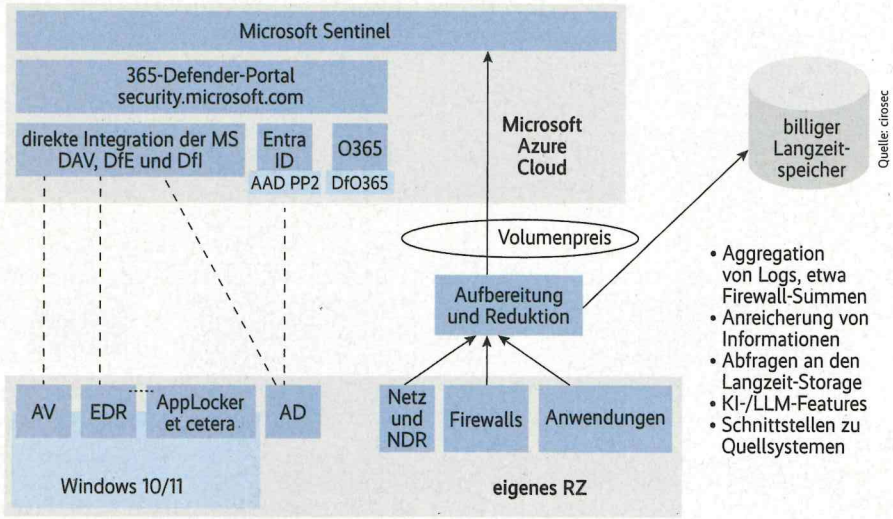
Risiken durch die Cloud

Auch die große Akzeptanz von Cloud-Computing verändert die IT-Welt stark und hat somit auch starke Auswirkungen auf die Informationssicherheit. Neue Schwachstellen in den Cloud-Angeboten kommen hinzu, für die es neue Sicherheitsprodukte gibt, die sie erkennen und beheben sollen. So gibt es neue Produkte zum Erkennen und Verhindern von Angriffen auf die Cloud-Dienste, neue Sicherheitsprodukte in der Cloud für althergebrachte Risiken oder neue Sicherheitsprodukte und Dienstleistungen, die durch den Wandel der IT-Architekturen möglich oder notwendig werden.

Bereits etabliert sind dabei die CSPM-Produkte (Cloud Security Posture Management), die Konfiguration und Härtung der Cloud-Infrastrukturen betrachten, bewerten und sicherheitsrelevante Änderungen vorschlagen. Noch relativ jung sind Pakete, die sich auf SaaS-Schwachstellen konzentrieren. Große SaaS-Produkte erlauben es in der Regel, dass Anwender anderen Personen Zugriffsrechte erteilen. Dafür bieten sie Schnittstellen zu anderen SaaS-Produkten an, für die man dann Access-Token oder andere Credentials hinterlegen kann. Die Sicherheit vieler dieser Mechanismen hängt von den Aktivitäten der Anwender ab. SaaS-Security-Produkte konzentrieren sich auf die großen SaaS-Angebote, analysieren ihre Freigaben, Schnittstellen oder konfigurierte Automatisierungen, um Schwachstellen erkennen und beheben zu können.

SaaS hat noch einen weiteren Markt geschaffen, bei dem es um die Sichtbarkeit und Verwaltung der Identitäten in SaaS-Applikationen geht. Oft nutzen die Mitarbeiter in einem Unternehmen nicht nur wenige große, ins zentrale Identity Management integrierte SaaS-Applikationen, sondern auch viele kleinere Applikationen mit eigener Rechte- und Benutzerverwaltung. Accounts bei Zoom, Slack, GitBook und vielen anderen werden vielleicht noch manuell angelegt und sind auch manuell wieder zu entfernen, wenn ein Mitarbeiter das Unternehmen verlässt. Moderne Identity-Governance-Produkte mit Fokus auf SaaS beginnen damit,

SOC-/MDR-Architekturen mit Log-Pipeline-Produkten



Log-Pipeline-Produkte können helfen, die volumenbasierten Cloud-Kosten für ein Cloud-SIEM im Griff zu behalten (Abb. 5).

dass sie die Nutzung von SaaS-Applikationen über verschiedene Wege erfassen, dann die Accounts und Lizenzen verwalten und somit sowohl einen Überblick schaffen als auch Abläufe automatisieren.

Weiterentwicklung bei SOC-Architekturen

KI und SaaS haben immer mehr Einfluss auf das Erkennen von Einbrüchen und auf die Architekturen in einem SOC. Mit der steigenden Popularität von XDR-Produkten, deren Management ohnehin in der Cloud liegt, und deren Weiterentwicklung zu SIEM-ähnlichen Services in der Cloud landen auch immer mehr Logdaten in der Cloud. Bei Microsoft mit Sentinel, bei Google mit Chronicle und bei vielen anderen Herstellern kann man das Wachstum gut beobachten. Entsprechend sind neue, externe SOC-Services entstanden, bei denen der SOC-Anbieter kein eigenes SIEM mehr für seine Kunden betreibt, sondern auf das SIEM des Kunden in der Cloud zugreift und dort seine Korrelationen durchführt. Für den Kunden hat das den Vorteil, dass er weniger abhängig vom SOC-Dienstleister wird und diesen einfacher austauschen kann, ohne dabei die Technik in seinem Cloud-SIEM ändert zu müssen. Der offensichtliche Nachteil ist aber, dass viele Logdaten nun in die Cloud gesendet werden und dort volumenabhängige Kosten verursachen.

Dies hat einen weiteren Trend erzeugt, sogenannte Log-Pipeline-Produkte, die Logdaten im Netz des Kunden sammeln, vorverarbeiten, filtern oder mit Zusatzdaten anreichern, um anschließend nur jene Logs in das Cloud-SIEM zu schicken, die für die Erkennung von Vorfällen wichtig sind. Andere Logs, die man nur für potenzielle forensische Untersuchungen aufbewahren möchte, werden stattdessen in einen billigeren Langzeitspeicher geschoben. Idealerweise kosten solche Lösungen weniger als der Transport der Logs in das Cloud-SIEM.

Selbstverständlich verwenden auch viele Log-Pipeline-Hersteller KI. Sei es, um unbekannte Logquellen zu normalisieren und in den Logs selbst zu erkennen, welche Spalten welchen Inhalt haben, oder um die eingegangenen Logs einem LLM zuzuführen, das dann unabhängig vom SIEM Fragen zu den Logs beantworten kann und die klassische Suche in einem SIEM zumindest teilweise ersetzt.

Wenn man vom SOC einen Schritt weiter an einen tatsächlichen Vorfall denkt, dann sollte dieser eingegrenzt und bearbeitet werden. Dabei sollten auch die Systeme forensisch analysiert werden. Nur auf diese Weise lässt sich hoffentlich rechtzeitig verhindern, dass ein kleiner Vorfall zu einer vollständigen Verschlüsselung der Unternehmensdaten und einer Erpressung führt. Oft gehen Unternehmen irrtümlich davon aus, dass es ausreicht, einen SOC-Service zu beauftragen, der dann auch Sofortmaßnahmen im Fall eines erkannten Incidents trifft. Doch ein SOC kann in der Regel nur einfache Sofortmaßnahmen wie das Isolieren eines PCs oder das Sperren eines Benutzeraccounts treffen. Größere Vorfälle, die forensische Untersuchungen oder eine Bearbeitung bei dem betroffenen Unternehmen vor Ort erfordern, sind die Domäne anderer Dienstleister, die garantierte Reaktionen im Bereich Incident Response und Forensik mit einem SLA anbieten.

Hier lauert jedoch das nächste Missverständnis, denn viele Unternehmen haben in den letzten Jahren Cyberversicherungen abgeschlossen, die oft die Unterstützung durch Spezialisten für Incident Response in ihrem Leistungsumfang enthalten. Daraus abzuleiten, dass man dann keinen eigenen Dienstleister mehr benötigt, wäre aber falsch, denn es häufen sich die Erfahrungsberichte, bei denen der von der Versicherung beauftragte und bezahlte Incident Responder nicht die Interessen des Opfers, sondern die Interessen der Versicherung vertreten hat. Bei Hinweisen auf Fehler des Opfers verweigerte die Versicherung die Zahlung. Entsprechend boomt auch der Trend zu dedizierten SLA-Verträgen mit spezialisierten Incident-Response- und Forensikexperten.

Fazit

Ständige Weiterentwicklungen in der Informationssicherheit lassen sich nicht aufhalten, denn die IT im Allgemeinen, die Angreifer, die gesetzlichen Vorschriften und auch der Markt entwickeln sich ständig weiter. Wer diese Entwicklung nicht mitgehen möchte, riskiert, zur leichten Beute für kriminelle Anbieter zu werden, da bisherige Schutzmaßnahmen ihre Wirksamkeit verlieren. Um dies zu verhindern, ist es nötig, immer am Ball zu bleiben, sich kontinuierlich über Trends und neue Entwicklungen zu informieren und diese im eigenen Organisationskontext fundiert zu bewerten. Denn gerade die Entwicklung der KI bringt neue Gefahren, aber auch Chancen bei der Abwehr mit sich. (avr@ix.de)

Quellen

[1] Hagen Molzer; Vishing: Angriffe per Telefon; iX 9/2025, S. 116
[2] Benjamin Häublein; ASPM: Angriffsfläche von Anwendungen reduzieren; iX 4/2025, S. 96
[3] Marco Bertenghi; Angriffe auf große Sprachmodelle; iX 1/2025, S. 42
[4] Udo Schneider; Agentic AI aus Securitysicht; iX 10/2025, S. 70
[5] Links zu den genutzten Statistiken und Top-10-Listen: ix.de/zf4s

STEFAN STROBEL

ist Buchautor sowie Gründer und Geschäftsführer des IT-Sicherheitshauses cirosec.