MANDIANT
NOW PART OF Google Cloud

Eine Momentaufnahme der Cybersicherheitslage – Ausgabe 3

„Der Vorteil des Verteidigers – Eine Momentaufnahme der Cybersicherheitslage“ greift Themen zur Cyberabwehr auf, die immer wichtiger werden, und liefert dazu passende Erkenntnisse aus Mandiant-Einsätzen und andere Praxisbeispiele. In dieser Ausgabe werden u. a. die folgenden Themen behandelt:

Der Weg zur passwortlosen Authentifizierung

In der Vergangenheit haben Unternehmen hauptsächlich die Challenge-Response-Authentifizierung mit einem einzelnen Passwort genutzt, um eine Identität für die Autorisierung zu prüfen. Dieses Modell einer einzigen Transaktion zur Authentifizierung ohne weitere Identitätsprüfungen konnte Unternehmen jedoch erheblichen Risiken aussetzen.

Während auf der einen Seite Angreifer immer ausgefeiltere Taktiken zum Hacken von Identitäten entwickelten, wurden auf der anderen Seite neue Kontrollmaßnahmen und Methoden zur Eindämmung von Risiken eingeführt. Die gängigste Kontrollmaßnahme, die viele Unternehmen ergriffen haben, ist die Durchsetzung der Multi-Faktor-Authentifizierung (MFA), wobei mindestens zwei unabhängige Methoden zur Identitätsprüfung kombiniert werden.

Im Rahmen zahlreicher Incident-Response-Untersuchungen konnte Mandiant beobachten, dass parallel zur verstärkten Nutzung herkömmlicher MFA in Unternehmen die Angreifer ihre Taktiken weiterentwickelten und sich mithilfe von Techniken wie den Folgenden Zugriff auf Identitäten verschafften:

Umgehung obligatorischer MFA

Missbrauch schwacher MFA-Methoden (z. B. SMS, Push-Benachrichtigungen, Telefonanrufe)

Übernahme der Kontrolle über Geräte für die MFA-Verifizierung und -Authentifizierung

Diese erhöhte Bedrohung rückte bei der durchgängigen MFA-Einführung neuere Lösungen mit stärkeren MFA-Methoden in den Fokus, wie etwa Zahlenabgleich, kontextbezogene Telemetrie-Benachrichtigungen und die Eingabe zeitlich begrenzter Einmalpasswörter. Daneben stärken Anbieter und Unternehmen MFA-Methoden weiter, indem sie Schlüssel/Token für FIDO2 (Fast Identity Online 2), Software-/Hardwaretoken für die Open Authentication (OAUTH) oder zertifikatsbasierte Authentifizierung nutzen.

Authentifikatoren

Zur weiteren Stärkung der Authentifizierungssicherheit fanden sogenannte Authentifikatoren Eingang in das Identitäts- und Zugriffsmanagement von Unternehmen. Authentifikatoren stellen eine Abkehr von einfachen Passwörtern dar, da sie mehrere Komponenten zur Bestätigung der Identität erfordern. Beispiele für Authentifikatoren sind u. a. ein Mehrfachansatz mit einem Benutzernamen/Passwort in Kombination mit starken MFA-Methoden, Zertifikaten, Kontext zum Gerätestatus, Berechnung des Identitätsrisikos oder auch passwortlose Methoden.

Durch eine Strategie mit Authentifikatoren wird das Gesamtrisiko infolge eines gestohlenen Passworts erheblich reduziert, da dieses nicht mehr als alleinige Authentifizierungsmaßnahme genügt.

Was bedeutet „passwortlos“?

Ansetzend bei starken MFA-Methoden erfolgt in vielen Unternehmen allmählich ein Übergang zur passwortlosen Authentifizierung im Rahmen einer Strategie, die auf Authentifikatoren setzt. Passwortlos ist im Grunde jede Methode zur Bestätigung der Identität, bei der kein geheimes Wissen erforderlich ist. Stattdessen erfolgt die Identifizierung mittels eines Geräts im Besitz der betreffenden Person oder eines ihrer physischen Merkmale (Biometrie). Bei passwortlosen Methoden erhöht die Einbeziehung eines gegenständlichen oder individuellen physischen Faktors die Sicherheit, da kein wissensbezogener Faktor (wie etwa ein Passwort) bei der Authentifizierung eine Rolle spielt.

Praktikable und skalierbare Methoden zur passwortlosen Authentifizierung umfassen u. a.:

- **Mobile Authentifikator-Anwendungen:** Diese können auf der Basis eines synchronisierten Algorithmus entweder eine Einmalkennung erzeugen oder genutzt werden, um eine Zahlenfolge, die dem Nutzer angezeigt wird, zu bestätigen oder abzugleichen.
- **FIDO2-basierte Hardwaretoken und Schlüssel:** Diese können entweder physisch, über Bluetooth oder mittels Nahfeldkommunikation (NFC) eine Verbindung zu einem Gerät herstellen. Speziell mit der FIDO2-WebAuthn-Methode kann das gerätegebundene Hardwaretoken zur Authentifizierung gegenüber der Zielanwendung genutzt werden. Dazu wird ein Paar aus einem eindeutigen kryptografischen Schlüssel, der auf dem mobilen Authentifikatorgerät gespeichert ist, und einem übermittelten öffentlichen Schlüssel verwendet. FIDO2 WebAuthn ist eine effektive Methode der passwortlosen Authentifizierung zur Bekämpfung von Phishing, Spoofing und Adversary-in-the-Middle-Angriffen (AitM).
- **Passkeys:** Diese funktionieren wie ein FIDO2-Token, wobei ein kryptografisches Schlüsselpaar erzeugt und lokal auf einem Mobilgerät gespeichert wird. Unter Verwendung von Verschlüsselung mit einem öffentlichen Schlüssel werden die Passkeys an die Anwendung übermittelt, bei der die Authentifizierung erfolgen soll und die den öffentlichen Schlüssel speichert. Für den Zugriff auf einen konfigurierten Passkey auf einem Mobilgerät ist entweder die biometrische Identifizierung oder eine PIN-Eingabe/Wischbewegung wie bei gängigen Mobilgeräten erforderlich.
- **Digitale Zertifikate:** Diese ermöglichen unter Verwendung von Paaren aus einem öffentlichem und einem privatem Schlüssel die Erzeugung einer gültigen digitalen Signatur der „Identität“ als Antwort auf eine Authentifizierungsanfrage. Auf modernen Geräten kann das Trusted Platform Module (TPM) als interner Authentifikator zum Speichern des privaten kryptografischen Schlüssels genutzt werden, der verwendet wird, um ein Zertifikat zu signieren, das für die „passwortlose“ Authentifizierung mit einem entsprechenden öffentlichen Schlüssel ausgestellt wird.

- **Biometrie:** Hierbei werden eindeutige physische Merkmale eines Menschen zur Bestätigung der Identität genutzt. Am gängigsten ist die biometrische Authentifizierung per Fingerabdruck (z. B. Touch ID und Fingerprint Unlock) oder Gesichtserkennung (z. B. Face ID und Face Unlock), die in viele Smartphones, Mobilgeräte und moderne Laptops integriert ist.

Planung der Einführung passwortloser Authentifikatoren

Herkömmliche Anwendungen und Infrastrukturen, die fortschrittliche Authentifizierungsmethoden nicht ohne Weiteres unterstützen, können ein Hemmschuh bei der einheitlichen Umsetzung des Ansatzes mit Authentifikatoren in Unternehmen sein. Anstatt sich auf die Einbindung jeder einzelnen Anwendung in diesen Ansatz zu konzentrieren, ist es zurzeit gängige Praxis, dass Unternehmen eine Single-Sign-on-Lösung (SSO) von einem Drittanbieter als erste Anlaufstelle für die Authentifizierung nutzen, die dann den authentifizierten Zugriff auf dahinter liegende Anwendungen vermittelt.

Die Einbindung passwortloser Authentifikatoren in das Gesamtkonzept will gut geplant sein, was Zeit in Anspruch nimmt. Sehr allgemein gefasst sollten die folgenden Überlegungen angestellt werden:

Identifizieren:

- aktuelle Technologien und Plattformen, die als Identitätsspeicher und Plattformen für die Autorisierung dienen
- vorhandene Identitätsspeicher, die nativ passwortlose Authentifizierungsmethoden unterstützen oder eine Integration durch einen Drittanbieter und Broker erfordern
- innerhalb eines Unternehmens bestehende Identitäten, einschließlich Identitätsarten, mit denen Sie den passwortlosen Ablauf testen und verifizieren könnten
- Ausgleichsmaßnahmen und fortschrittliche Methoden zur Erkennung von Identitätsarten, die keine passwortlosen oder starken Authentifizierungsmethoden unterstützen (z. B. Programm-/Servicekonten)
- Auswirkungen auf Gast-/Drittanwender, die möglicherweise nicht in die passwortlose Authentifizierung eingebunden werden können
- Geräte, die Anwender aktuell für die Authentifizierung und den Zugriff nutzen, und Prüfung, ob diese Geräte passwortlose Methoden unterstützen
- Anwendungen, die direkt in die passwortlose Authentifizierung eingebunden werden können, oder Anwendungen, die die SSO-Verbindung mit der Plattform eines Drittanbieters unterstützen, die passwortlose Methoden ermöglicht

Planen:

- Beschaffung und sichere Bereitstellung und Implementierung von Geräten, die die passwortlose Authentifizierung unterstützen
- Schulung der Nutzer zur passwortlosen Praxis
- Modifikation der Konfiguration von Identitätsspeichern und Geräten zur Implementierung der passwortlosen Integration
- Tests und Validierung der passwortlosen Integration mit Pilotnutzern und ausgewählten Anwendungen
- Ersteinführung und Nutzereinbindung sowie die Ausweitung der passwortlosen Authentifizierung auf das gesamte Unternehmen

Eine weitere wichtige Überlegung im Zusammenhang mit der passwortlosen Authentifizierung ist die Anpassung der Wiederherstellungsschritte, wenn ein Gerät oder Schlüssel verloren geht oder gestohlen wird, da dies nun zentrale Elemente im Authentifizierungsprozess für eine Identität sind. Die Planung sicherer Wiederherstellungsschritte muss nicht nur ein Abwägen der unternehmerischen Risiken umfassen, sondern auch des Pro und Contra in Bezug auf die Benutzereinbindung und die Self-Service-Fähigkeit insgesamt.

Interne Authentifikatoren (z. B. Geräte mit einem integrierten TPM) können zwar die Möglichkeit bieten, private Schlüssel zu exportieren (speichern) oder zwischen Geräten zu synchronisieren, doch dies kann auch mit einem Risiko verbunden sein, wenn die Schlüssel nicht ordnungsgemäß geschützt und gespeichert werden. Bei der Nutzung von Drittanbietern zur Identitätsbereitstellung können auch Wiederherstellungsschlüssel und -formulierungen in Betracht gezogen werden, um eine passwortlose Identität zur Einrichtung auf einem neuen Gerät wiederherzustellen. Wenn zur passwortlosen Authentifizierung mobile Authentifikatoren verwendet werden, kann der Versand von Validierungsnachrichten an ein Mobilgerät oder eine E-Mail-Adresse eine Option zur Identitätswiederherstellung sein.

Die Umstellung von einfachen Passwörtern auf die passwortlose Authentifizierung ist ein langer Weg. Viele Unternehmen, die sich für Authentifikatoren entschieden haben, haben festgestellt, dass eine starke MFA ein guter Anfang ist, um das Fundament für die passwortlose Authentifizierung zu legen. Während der Weg dorthin sorgfältiger Planung, Ausführung und Prüfung bedarf, sind die Vorteile hinsichtlich Sicherheit und Risikominderung immens, zumal in modernen hybriden Betriebsmodellen die Identität die neue Abwehrlinie darstellt.

Risikominimierung zum Erwerben einer Cyberversicherung

US-Banken ermittelten im Jahr 2021 Transaktionen in Zusammenhang mit Ransomware in Höhe von 1,2 Milliarden US-Dollar bei 1.489 Meldungen an Regulierungsbehörden – ein steiler Anstieg gegenüber 416 Millionen US-Dollar bei 487 Meldungen im Jahr davor.[4]

Ransomware-Zahlungen haben sich im Zeitraum 2020–2021 mehr als verdoppelt[1], wodurch Versicherer größere Verluste hinnehmen mussten und der Markt für die Absicherung von Cyberrisiken starken Schwankungen ausgesetzt war. Erst in jüngerer Zeit trat wieder eine Stabilisierung ein. Doch auch wenn der Anstieg der Versicherungsprämien gegen Ende 2022 um 80 % zurückging, wodurch sich die Marktaussichten für 2023 verbesserten[2], gehen die meisten Versicherungsträger davon aus, dass die Cyberrisiken weiterhin zunehmen werden, da Ransomware-Forderungen eine Hauptbedrohung bleiben[3]. Infolgedessen müssen sich Unternehmen beim Abschluss einer Versicherung auf eine verschärfte Prüfung ihrer Sicherheitsmaßnahmen und internen Prozesse und Abläufe bezüglich Cyberrisiken einstellen. Außerdem bleiben für weit verbreitete Ereignisse (d. h. Log4j) und für Vorfälle, die zu dem Krieg in der Ukraine oder staatlich geförderten Angreifergruppen zurückverfolgt werden können, besorgniserregende Ausnahmen bestehen. Versicherungsträger senken auch weiterhin die Deckungssummen für Schäden durch Ransomware oder schließen solche Schäden gänzlich aus, wenn ein Unternehmen nicht nachweisen kann, dass es über angemessene Kontrollmaßnahmen zur Eindämmung dieses Risikos verfügt.

Im Verlauf der letzten zwölf Monate hat Mandiant eine wachsende Beteiligung von Versicherern von Cyberrisiken bei Incident-Response-Einsätzen beobachtet. CISOs werden bei Entscheidungen über die von einer Versicherung abzudeckenden Risiken nicht konsistent hinzugezogen, doch empfehlen wir, dass sie eng mit dem Risikomanager und den Rechtsberatern des Unternehmens zusammenarbeiten, um Genauigkeit während des Antragsverfahrens sicherzustellen und die Policen zu prüfen, damit es bei einem Sicherheitsvorfall nicht zu bösen Überraschungen kommt.

Grundlagen der Cyberversicherung

Mitte der Nullerjahre begannen Versicherer, die Kosten durch Cyberangriffe, die sich direkt auf das Geschäft des betroffenen Unternehmens auswirkten, in die Deckung einzuschließen.[5] Seitdem hat sich die erweiterte Deckung zu einem nützlichen Instrument entwickelt, mit dem Finanzrisikomanager und führende Cybersicherheitsanbieter Risiken mindern und die Kosten infolge von Datenlecks und anderen Sicherheitsvorfällen ausgleichen. Policen decken im Allgemeinen Cyberrisiken für das Unternehmen (Eigenrisiko) und Schadensersatzforderungen von Verbrauchern oder anderen Unternehmen (Haftungspflicht gegenüber Dritten) ab. Zu Anfang deckten Cyberversicherungen vorwiegend die durch Datenlecks entstandenen Kosten ab und Unternehmen mussten den Versicherern gegenüber darlegen, welche Art von Dokumenten, Kundendaten und regulierten Daten sie verarbeiteten, und ihre Einhaltung von Regulierungsstandards wie HIPAA und PCI DSS belegen. Ransomware-Angriffe und mehrgleisige Erpressungsversuche bergen zusätzlich das Risiko einer Geschäftsunterbrechung, die Geschäfte zugrunde richten und erhebliche Kosten verursachen kann.

1. Wall Street Journal, „Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says", 4. November 2022.
2. Marsh, „US Cyber Insurance Market Update: Signs of improvement in third quarter of 2022", 7. Oktober 2022.
3. Woodruff Sawyer, „2023 Property & Casualty Looking Ahead Guide", 10. Januar 2023.
4. Wall Street Journal, „Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says", 4. November 2022.
5. The Federal Reserve Bank of Chicago, Chicago Fed Letter, No. 426, 2019, „The Growth and Challenges of Cyber Insurance", 2019.

TABELLE 1: Gängige abgedeckte Cybersicherheitsrisiken

Deckung von Eigenrisiko	Haftungspflicht gegenüber Dritten
Kosten für Incident Response und forensische Untersuchungen	Schadensersatzforderungen aus Sicherheit und Datenschutz
Benachrichtigung, Kredit- und Identitätsüberwachung	Schadensersatzforderungen aus Multimedia-/ Medienkommunikation
Datenwiederherstellung	Behördlich verhängte Strafzahlungen
Geschäftsunterbrechung	Schadensersatzforderungen aus PCI DSS
Cybererpressung und Cyberkriminalität	Strafzahlungen aufgrund des Telephone Consumer Protection Act
Rufschädigung	

* Quelle: Honigman LLP Attorneys and Counselors, „Cyber Insurance 101", 19. Mai 2021.

Infolgedessen haben Versicherer ihre Bleistifte gespitzt und nehmen die technischen Kontroll- und Begrenzungsmaßnahmen von Unternehmen gegen Unterbrechungen und andere damit zusammenhängende geschäftliche Verluste genauer unter die Lupe. Die Folge ist eine rigorose Prüfung des versicherten Risikos und der Prämienkalkulation. Bis zum Abschluss einer Versicherung sind zusätzliche Fragen, Gespräche und Prüfungen der Umgebung durch einen externen Gutachter zu absolvieren.

Beth Burgin Waller, Vorsitzende der Praxis für Cybersicherheit und Datenschutz bei Woods Rogers, die neben ihrer Beratungstätigkeit zur Bedrohungsabwehr einen erheblichen Teil ihrer Zeit mit der Prüfung und Verhandlung von Cyber-versicherungen für ihre Klienten verbringt, empfiehlt, bei der Vorbereitung der Verhandlungen mit Versicherern das Risikomanagementteam und die Rechtsabteilung im eigenen Haus mit ins Boot zu holen.

Fragebögen im Verlauf des Prozederes enthalten oft Schwarz-Weiß-Fragen, die modernen komplexen Unternehmensinfrastrukturen mit mehreren Clouds und Netzwerken nicht gerecht werden. Bei einer Frage, ob im gesamten Unternehmen Multi-Faktor-Authentifizierung (MFA) umgesetzt ist, verlangen Versicherer möglicherweise Belege dafür, dass MFA in allen Bereichen des Unternehmens vorhanden ist – von Backups über cloudbasierte Geschäftsanwendungen bis hin zum VPN. Ihr Team für Beratung und Risikomanagement kann pauschale Aussagen im Antrag identifizieren und ergänzende Erläuterungen zu aktuellen Produktionskontrollen und etwaigen Verbesserungsplänen beitragen.

Die Feinheiten der IR-Abdeckung

Burgin Waller empfiehlt unbedingt, die Musterpolice gründlich zu lesen. „Mit der Stabilisierung des Marktes entwickelt sich auch bei Policen für Cyberversicherungen eine Standardsprache, ähnlich wie bei anderen Versicherungsprodukten", sagt sie. Die Musterpolice kann ergeben, dass für die Deckung für Geschäftsunterbrechungen ein bestimmtes Limit gilt, aber ohne die gründliche Lektüre der Musterpolice enthält Ihr Vertrag am Ende möglicherweise Ausschlussklauseln für veraltete Software, weit verbreitete Ereignisse wie Log4j oder – ganz aktuell – Kriegshandlungen, die Vorfälle betreffen, die staatlichen Akteuren zugeschrieben werden. Burgin Waller rät, insbesondere auf Entschädigungsgrenzen zu achten. In einem Beispielfall enthielt eine Basis-Cyberversicherung eine Entschädigungsgrenze für Vorfälle, die über Phishing eingeleitet wurden, und erwartete, dass das Unternehmen für Ransomware eine ergänzende Versicherung abschloss. Burgin Waller erläutert: „Die sorgfältige Lektüre der Musterpolice gleich zu Beginn kann Ihnen erhebliche Kopfschmerzen ersparen, weil Sie darüber informiert sind, für welche Schäden Deckung besteht (oder nicht), bevor der Versicherungsfall eintritt."

Kann man davon ausgehen, dass die Kosten für den Incident-Response-Anbieter und damit zusammenhängende Kosten abgedeckt sind? Die Incident-Response-Experten von Mandiant begegnen in der Praxis drei gängigen Szenarien:

1) Der IR-Dienstleister ist ein genehmigter Anbieter mit vorab ausgehandelten Tarifen. Das vereinfacht die Beauftragung im Ernstfall und kann die Geltendmachung von Ansprüchen gegenüber der Versicherung vereinfachen.
2) Der IR-Dienstleister wurde nicht vorab genehmigt und der Versicherer übernimmt die Kosten bis zu einem bestimmten Stundensatz. Der Versicherungsnehmer muss für die Differenz aufkommen, wenn der IR-Tarif höher liegt als die abgedeckte Summe.
3) Der IR-Dienstleister wurde nicht vorab genehmigt und der Versicherer übernimmt keinerlei Kosten, wenn dieser IR-Dienstleister beauftragt wird. Dieses Szenarium kann im Falle eines Datenverstoßes die größten Störungen verursachen.

Es ist wichtig, die Musterpolicen im Hinblick auf die Deckung des gesamten Incident-Response-Prozesses zu prüfen. Manche Policen decken nur die Untersuchung ab und schließen Ransomware-Zahlungen, allgemeine Beratungskosten oder Kosten für die Wiederherstellung und langfristige Schadensbehebung aus. Außerdem umfasst die Deckung bei manchen Versicherungsträgern möglicherweise nicht die vollständige Untersuchung zur Ermittlung des genauen Angriffsweges und die Prüfung, dass keine Backdoors eingerichtet wurden, über die der Versicherungsnehmer leicht erneut infiziert werden könnte. An diesem Punkt wird die Frage, ob mit einer gründlichen Untersuchung mit dem Ziel, künftige Risiken zu reduzieren, fortgefahren werden soll, zu einer Geschäftsentscheidung.

Ein neuer Ansatz

Allgemein reift der Markt für Cyberversicherungen und Anbieter arbeiten mit ihren Kunden zusammen, um die Widerstandsfähigkeit gegenüber Cyberrisiken insgesamt zu stärken. Die Versicherungsbranche verfügt über sehr ausgereifte Risikomodellierungsprogramme, die zur Stärkung der Sicherheit von Unternehmen genutzt werden.

Viele Versicherungspartner nutzen eine Reihe von geprüften Anbietern und Lösungen, um ihre Kunden dabei zu unterstützen, sich auf dem Markt für Cybersicherheit zurechtzufinden und ihr Risiko durch den Einsatz von Technologie zu reduzieren, deren Wirksamkeit bewiesen ist.

Versicherungspartner haben sogar Sicherheitsmaßnahmen ermittelt, die das Cyberrisiko von Unternehmen und die damit verbundenen Versicherungsprämien positiv beeinflussen können.[6] Mandiant unterstützt Empfehlungen aus der Versicherungsbranche und möchte die folgenden fünf Praktiken besonders hervorheben, die bei richtiger Umsetzung die Folgen typischer Angriffe mindern oder gängige Angriffe gänzlich unterbinden können:

1. **Multi-Faktor-Authentifizierung:** MFA oder Mehrfaktor-Authentifizierung ist eine Technologie, die zur Erlangung des Nutzerzugangs zwei bzw. mehr voneinander unabhängige Authentifizierungsformen miteinander kombiniert (z. B. Passwörter, Sicherheitstoken und Gesichtserkennung oder Fingerabdruck). Im Rahmen zahlreicher Incident-Response-Untersuchungen konnte Mandiant beobachten, dass parallel zur verstärkten Nutzung herkömmlicher MFA in Unternehmen die Angreifer ihre Angriffstaktiken weiterentwickeln, um sich Zugriff auf Identitäten zu verschaffen. Die Einführung starker MFA-Tools und -Methoden, wie Zahlenabgleich, kontextbezogene Telemetriebenachrichtigungen und die Eingabe zeitlich begrenzter Einmalpasswörter, über alle von außen zugänglichen Log-in-Portale hinweg und für sämtliche sensiblen internen Anwendungen kann das Risiko durch gängige Techniken von Angreifern für den ersten Zugriff senken.
2. **Verwaltung von Identitäten und Zugriffsrechten:** Die Identität ist in modernen hybriden Betriebsmodellen die neue Abwehrlinie. Mandiant beobachtet bei vielen Incident-Response-Einsätzen, dass in Systeme für die Verzeichnis- und Zugriffsverwaltung eingedrungen wurde. Oft nutzen die Angreifer diese Systeme dann, um Zugriffsrechte auszuweiten. Unternehmen müssen dafür Sorge tragen, dass Benutzer und Systeme die ordnungsgemäßen Zugriffsrechte haben und dass Systeme für die Verzeichnis- und Zugriffsverwaltung ordnungsgemäß konfiguriert sind, sodass eine unbefugte Ausweitung besonderer Zugriffsrechte unterbunden wird.
3. **Gesicherte, verschlüsselte und getestete Backups:** Mandiant empfiehlt Unternehmen, einen geprüften Plan für die Sicherung und Verschlüsselung von Backups festzulegen, um die Wiederherstellung von Systemen und Daten im Falle eines Cyberangriffs zu erleichtern. Lösungen für Backups und externe Speicherung können dazu beitragen, die Wahrscheinlichkeit eines Verlustes von geistigem Eigentum zu senken und sicherzustellen, dass wertvolle Daten und Dokumente vor Verlust geschützt sind. Unternehmen nutzen in zunehmendem Maße Cloud-Service-Lösungen zur Aufbewahrung einer Kopie ihrer Cloud- oder Hybridnetzwerke für den Fall eines Cyberangriffs, der anderenfalls den Betrieb zum Stillstand brächte.

6. Marsh, „Cyber Insurance Market Overview: Fourth Quarter 2021", 7. Dezember 2021.

4. **Pläne und Tests zur Abwehr von Cybersicherheitsvorfällen:** Nach Ansicht von Mandiant sind Pläne und Tests zur Abwehr von Cybersicherheitsvorfällen eine wichtige Maßnahme, die u. a. die Überprüfung bestehender technischer Kontrollen, Netzwerkarchitekturen und Erstabwehrfähigkeiten umfasst. Mandiant rät zur Erstellung eines Plans für typische Abwehrszenarien und zur kontinuierlichen Überprüfung der Fähigkeiten zur Cyberabwehr, um einen etwaigen Sicherheitsvorfall schnell eindämmen zu können.
5. **Externe Partner für Rechtsfragen und Incident Response:** Ein wichtiger Aspekt bei der Planung zur Abwehr von Cybersicherheitsvorfällen ist die Bereitschaft, Unterstützung von außen hinzuzuziehen, um das Unternehmen vor rechtlichen Risiken zu schützen und bei der Bedrohungsabwehr Experten mit ins Boot zu holen. Rechtsberater, insbesondere mit dem Schwerpunkt Cyberrecht, sollten in der Lage sein, im Falle eines Angriffs nahtlos mit forensischen Ermittlern zusammenzuarbeiten, um die rechtliche Haftbarkeit und Risiken zu beurteilen, die aus dem Vorfall hervorgehen könnten. Externe Unterstützung bei der Bedrohungsabwehr kann die Reaktionszeit maßgeblich verkürzen und so die Folgen eines Datenverstoßes mildern. Ein Incident-Response-Bereitschaftsdienst (Incident Response Retainer; IRR) ermöglicht es Unternehmen, grundlegende Bedingungen für Incident-Response-Services zu vereinbaren, bevor der Verdacht auf einen Sicherheitsvorfall besteht.

Zudem bieten die meisten Versicherungspartner Sicherheitsberatung und -services zur Unterstützung beim Antragsverfahren an. Viele Versicherungsmakler und -träger bieten ein differenziertes Serviceangebot, das neben der Beratung auch Beurteilungen, Cyberhygiene und Prozesse umfasst, die zur Entwicklung einer effektiven Abwehr erforderlich sind.

Weitere Hilfe rund um das Thema Cyberversicherung bieten die Partner, Podcasts und Webinare von Mandiant sowie die Angebote der Google Cyber Risk-Teams.

Fallstudie: Sicherheitsanalysten erkennen und stoppen Angriffe auf die Softwarelieferkette

Was Sie bei der Aktivierung der Funktionen zur Bedrohungserkennung und -abwehr erwarten sollten

Letztes Jahr berichtete Mandiant über eine signifikante Zunahme von erfolgreichen Angriffen auf Lieferketten: 2021 nahmen 17 Prozent der Einbrüche in IT-Systeme ihren Anfang in der Lieferkette. Im Jahr davor lag dieser Anteil bei unter einem Prozent.[7] Der Anstieg lässt sich zum Teil dadurch erklären, dass 86 Prozent der von Mandiant verfolgten Angriffe im Zusammenhang mit der SolarWinds-Kampagne und SUNBURST standen.[8] Allerdings korreliert er auch damit, dass Unternehmen im Durchschnitt mit 244 Lieferanten auf technischer Ebene verbunden sind.[9]

Angriffe auf Softwarelieferketten sind nichts Neues. Im Jahr 2017 erschütterte NotPetya die Welt. Dieser als Ransomware getarnte Schadcode nutzte die geleakte NSA-Schwachstelle EternalBlue aus, infiltrierte Netzwerke und zerstörte dann systematisch Daten. Die Angreifer hinter NotPetya hackten den Hersteller einer Software für den Finanzsektor, der auch ukrainische Behörden auf seiner Kundenliste führte.

Im gleichen Jahr wurde das Dienstprogramm CCleaner[10] gehackt. Die Kriminellen konnten die echte Version der Software gegen eine manipulierte Version austauschen, wodurch sie Zugriff auf über zwei Millionen Hosts erhielten.

2020 kam es zu dem oben bereits erwähnten weitläufigen Angriff mittels einer Komponente von SolarWinds, hinter dem APT29 (vormals UNC2452) steckte – eine Hackergruppe, deren Zielauswahl einer Beurteilung zufolge mit strategischen Interessen Russlands übereinstimmt.[11] Zu den Opfern von APT29 zählten auch staatliche Organisationen und Fortune-500-Unternehmen. Einmal mehr zielten Angreifer auf die Softwarelieferkette ab, als sie einen Backdoor-Code in die Softwarekomponente Orion einschleusten, mit dem sie Zugang zur inneren Umgebung der Betroffenen erhielten. Dadurch konnten sie die Malware SUNBURST installieren, nachdem der manipulierte Code über einen legitimen Prozess verteilt worden war.

Die Angreifer haben einen Weg gefunden, das Fundament unserer digitalen Geschäftswelt zu manipulieren. Indem sie ein beliebtes, von Softwareentwicklern genutztes Paket hacken, fällt es ihnen im weiteren Verlauf leicht, den Schadcode in großem Maßstab direkt an die Opfer zu verteilen. Dieser Ansatz wirft bei den Verteidigern die Frage auf, ob wir uns unserer Abwehrbereitschaft wirklich gewiss sind. Unternehmen auf der ganzen Welt tun alles Erdenkliche, um ihre Angriffsfläche stets im Blick zu behalten und sich weiterhin auf ihre Erkennungs- und Abwehrfunktionen verlassen zu können. Doch allzu oft sind Unternehmen sich bezüglich ihrer Fähigkeit, Cyberangriffe in ihrer Softwarelieferkette schnell erkennen und aufhalten zu können, nicht sicher. Das liegt zum Teil daran, dass sie nicht über entsprechend ausgebildete Abwehrexperten verfügen und dass sie nicht oft genug aktiv werden, um die interne Expertise auszubauen und zu verfeinern.

7. Mandiant, M-Trends 2022
8. Mandiant, M-Trends 2022
9. Mandiant, „Der Vorteil des Verteidigers – Eine Momentaufnahme der Cybersicherheitslage, Ausgabe 2", 2022.
10. Mandiant Threat Intelligence, „CCleaner Supply-Chain Compromise Possibly Linked to Chinese Cyber Espionage Operators", September 2017.
11. Mandiant, „Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor", Dezember 2020.

Manipulationen entlang der Softwarelieferkette setzen darauf, das Vertrauen in Drittanbieter auszunutzen, um sich indirekt Zugang zur Umgebung eines Opfers zu verschaffen. Daher sind sie oft nur schwer aufzuspüren. Letztendlich sind der geschulte Blick des Sicherheitsanalysten und der Untersuchungsprozess die entscheidenden Faktoren bei der Identifizierung und Abwehr ausgereifter Angriffe.

> Bei einem Angriff über die Lieferkette erschwert das bestehende Vertrauen die direkte Erkennung des infiltrierten Schadcodes besonders. Die aktive und effektive Fähigkeit zur Bedrohungserkennung und -abwehr wird noch bedeutsamer, da ein in den späteren Stadien eines Angriffs festgestelltes verdächtiges Ereignis den Analysten die Möglichkeit gibt, die Manipulation indirekt aufzuspüren, indem sie die Aktivitäten der Angreifer durch die Untersuchung rückwärts verfolgen.
>
> **– Steve Ledzian VP, CTO-APAC, Mandiant**

Analysten erkennen und untersuchen die Manipulation einer Softwarelieferkette

Beginnend Mitte Oktober 2021 bemerkten Sicherheitsanalysten des Managed Service zur Bedrohungserkennung und -abwehr von Mandiant mehrere Ereignisse, bei denen es sich anscheinend um die Einschleusung falscher Daten in Open-Source-Repositorys handelte. Der folgende Fall beschreibt ihren Erkennungs- und Untersuchungsprozess, einschließlich der Fragen, die sie sich dabei stellten. Unter anderem wurden bei diesem Prozess auch Pakete auf Node Package Manager (NPM) gehostet, dem Paketmanager für die JavaScript-Plattform Node.js.

Ein kleines Team von Mandiant-Sicherheitsanalysten stellte anfangs mehrere Warnmeldungen fest, die darauf hinwiesen, dass das native Windows-Dienstprogramm **CERTUTIL.EXE** genutzt wurde, um Schadcode von einer gängigen URL **(hxxps://citationsherbe[.]at/sdd.dll)** herunterzuladen. Als weitere Analysten im Security Operations Center (SOC) ähnliche Warnmeldungen erhielten, begann das Team mit einer koordinierten Aufklärung anhand von Leitfragen, auf die sie im Laufe der Untersuchung Antworten fanden.

Worum handelt es sich? Wie wurde es in das System heruntergeladen?

Die ersten Leitfragen bei der Untersuchung sind „Welche Malware liegt vor und was kann sie?“ sowie „Wie ist sie ins System gelangt?“. Die Analysten besorgten sich die Malware von den ersten Hosts, um die Funktionen und Fähigkeiten des verdächtigen Codes zu ermitteln. Eine erste Analyse ergab, dass es sich dabei um eine Variante der Malware DANABOT handelte, die auf den Diebstahl von Anmeldedaten durch Kommunikation mit einem angreifergesteuerten Command-and-Control-Server (C2-Server) abzielt. Unter Verwendung der C2-Adresse der Malware begannen die Analysten damit, die Umgebung weiter zu durchkämmen und andere Systeme zu identifizieren, die mit der Infrastruktur der Angreifer kommunizierten. Durch diesen Prozess konnten die Analysten bestimmen, ob die gleiche oder eine ähnliche Malware in andere Systeme eingeschleust worden war, ohne eine entsprechende Warnmeldung auszulösen. Sobald sich der Verdacht auf Malware bestätigt hatte, fing das Analystenteam an, die betroffenen Hosts per Fernwartung abzuschirmen bzw. das Incident-Response-Team einzuschalten.

DANABOT ist eine in Delphi verfasste Backdoor, die mit einem speziellen Binärprotokoll über TCP kommuniziert. Diese Backdoor implementiert ein Plug-in-Framework, mit dem sie über heruntergeladene Plug-ins weitere Funktionen hinzufügen kann. Zu den Funktionen von DANABOT zählen u. a. die vollständige Systemkontrolle über ein VNC- oder RDP-Plug-in, Video- und Screenshot-Erfassung, die Aufzeichnung von Tastatureingaben, die willkürliche Ausführung von Shell-Befehlen und die Übertragung von Dateien. Mit seinem Proxy-Plug-in kann DANABOT Netzwerkverkehr in Zusammenhang mit den anvisierten Websites umleiten oder manipulieren. Diese Funktion wird oft genutzt, um an Anmelde- oder Bezahldaten zu gelangen. Außerdem kann DANABOT gespeicherte Anmeldedaten für Webbrowser und FTP-Clients ausschleusen.

„**ua-parser-js**" ist ein Paket mit kleinem Formfaktor, das wenig Ressourcen in Anspruch nimmt und in einer Webanwendung oder serverseitigen Anwendung implementiert wird, um die relevanten Daten zu extrahieren und herauszufiltern, die zum Parsen eines Nutzer-Agent-Strings (d. h. Browser, Engine, Betriebssystem, CPU und Gerät) notwendig sind.

Wie konnten die Angreifer eindringen?

Um nachvollziehen zu können, wie die Malware eingeschleust wurde, untersuchen Analysten typischerweise Daten, die von Technologie für die Bedrohungserkennung und -abwehr am Endpunkt (EDR) erfasst werden. Anhand der EDR-Telemetriedaten konnten die Analysten die Aktivität zu legitimen Befehlen zurückverfolgen, die von Anwendern ausgeführt wurden, um NPM-Pakete zu aktualisieren.

Eine gründliche Untersuchung ergab, dass auf jedem der betroffenen Hosts eine ähnliche Datei im Verzeichnis **UA-PARSER-JS PACKAGE** gespeichert war, weswegen den Analysten der Verdacht kam, dass dieses Verzeichnis manipuliert war und die Malware verteilte. Durch die schädliche Änderung an dem JS-Package-Verzeichnis war der Installation des Pakets ein Schritt vorgeschaltet worden, in dem die Malware heruntergeladen wurde. Bei der näheren Untersuchung des manipulierten Skripts stellten die Analysten fest, dass es auch Coinminer (auch als Kryptowährungsminer bekannt) auf den Host herunterlud. Die Analysten prüften die GitHub-Issues für das Paket-Repository und stießen auf die Frage eines Nutzers, ob das Paket vor Kurzem manipuliert worden sei. Einem GitHub-Issue vom 22. Oktober 2021 zufolge war um ungefähr 12:15 Uhr UTC das NPM-Paket „**ua-parser-js**", eine beliebte Node.js-Bibliothek mit mehr als sieben Millionen Downloads pro Woche, manipuliert worden, um Malware zu verbreiten. Dem Angreifer war es gelungen, drei Schadversionen des Pakets zu veröffentlichen, indem er das NPM-Konto des Autors gehackt hatte. Laut dem Git-Log des Repositorys stellte der Autor des Pakets am 22. Oktober zwischen 16:14 und 16:25 Uhr UTC eine saubere Version des betroffenen Pakets ein, um die weitere Verbreitung der Malware zu unterbinden.

Welche anderen Aktivitäten wurden von dem Angreifer ausgeführt?

Nachdem die Hosts abgeschirmt worden waren, setzten die Analysten ihre Untersuchung fort, um die Kernursache des Angriffs zu ermitteln. Bei einer Überprüfung des Git-Logs des Paket-Repositorys fanden anhand von Zeitstempeln heraus, wann die schädliche Veränderung gepusht und wann wenige Stunden später die Korrektur durchgeführt worden war. Durch eine weitere Analyse der Taktiken, Techniken und Prozesse (TTP) des Angreifers konnte das Analystenteam Verbindungen zu weiteren NPM-Paketen, die von demselben Angreifer manipuliert worden waren, herstellen und das Ausmaß von dessen Aktivität abschätzen. Das Team konnte die Aktivität mit ziemlicher Sicherheit der Hackergruppe UNC3379 zuordnen, die Malware analysieren, das Angreiferverhalten dokumentieren und Erkennungstechniken entwickeln, die zukünftige Aktivitäten im Keim ersticken.

Weitere Informationen zu diesem Angriff über eine Softwarelieferkette enthält der Artikel in unserem Forschungsblog „Bohrplattform: Lieferkettenangriffe über Node.js".

Vertrauen in den Instinkt, das kritische Denken und die Erfahrung von Analysten

Unabhängig vom Umfang der Untersuchung ist Zeit der entscheidende Faktor. Bei Mandiant verlassen wir uns bei der Untersuchung und Abwehr auf das Wissen, das fachliche Training und das kritische Denken unserer Analysten. Unsere Mitarbeiter gehen wie Detektive vor, die anhand von Hinweisen, Beweisen und forensischen Artefakten den Ablauf und Hintergrund hinter jedem Vorfall aufdecken. Das Ziel des Untersuchungsprozesses ist es, Schlüsselfragen zu dem Angriff zu beantworten, um die folgenden Punkte zu klären:

- Umfang der Infiltration
- Ob der Angriff immer noch andauert
- Frühester Zeitpunkt und Ursache des Eindringens
- Art und Umfang der betroffenen Daten
- Identität und Motive des Angreifers

Die Kenntnis dieser Fakten zu dem Angriff steckt den Rahmen für die Eindämmung, Beseitigung und Wiederherstellung ab. Mandiant empfiehlt, dass Sie Ihre Analysten durch Erfahrungen an vorderster Front, Simulationen und Schulungen dazu befähigen, Untersuchungen zu leiten und zentrale Entscheidungen bezüglich des Zeitpunkts und der Durchführung von Eindämmungs- und Beseitigungsmaßnahmen zu treffen. „Es ist nicht ungewöhnlich, dass Unternehmen, die Vorfälle selbst untersuchen und abwehren, vorschnell mit der Schadensbehebung beginnen", sagt Eric Scales, Vice President von Mandiant. „Je mehr man aber über den Angriff weiß, desto größer ist der Erfolg bei der Beseitigung und Wiederherstellung."

In dem hier dargestellten Fall wurden im Zuge der Untersuchung durch das MDR-Team von Mandiant wichtige seismische Indikatoren bezüglich der Aktivität entwickelt. Die Analysten führten eine erste Untersuchung (Triage) der eingeschleusten Malware durch, um geeignete Beseitigungsmaßnahmen zu bestimmen, und konnten auf der Grundlage ihres tiefgreifenden Wissens und der Forschung über die Hackergruppe erfolgreich eine Beurteilung der Umgebungen unserer Kunden vornehmen. Dadurch wurden weitere schädliche Aktivitäten in Zusammenhang mit dieser Kampagne entdeckt, die die kundenseitigen EDR-Produkte nicht erkannt hatten.

Aktivierung der Cyberabwehr im Rahmen der sektorübergreifenden, von der CISA gesetzten Leistungsziele für Cybersicherheit

Staatlich gesponsorte Angreifer haben nach wie vor kritische Infrastrukturen im Visier. Im letzten Jahr berichtete Mandiant über den Fund maßgeschneiderter Tools, mit denen Angreifer bestimmte industrielle Steuerungssysteme (ICS) oder Geräte für die Überwachung, Steuerung und Datenerfassung (SCADA) aufspüren, hacken und steuern können, sobald sie sich Zugriff auf ein OT-Netzwerk verschafft haben.[12] Da industrielle und kritische Infrastrukturen zunehmend vernetzt werden, verstärkt dieser erhöhte Entwicklungsstand der Bedrohungen die Notwendigkeit, dass Leitlinien für die Cybersicherheit kritischer Infrastrukturen auf dem aktuellen Stand sind. Die Cybersecurity and Infrastructure Agency (CISA), das National Institute of Standards and Technology (NIST) und die Gemeinschaft der Behörden und Organisationen haben Ziele für die Cybersicherheit ausgearbeitet, die für alle Sektoren kritischer Infrastrukturen gelten.

Im Oktober 2022 gab die CISA die „Cross-Sector Cybersecurity Performance Goals" (CPG; sektorübergreifende Leistungsziele für die Cybersicherheit)[13] heraus. Sie dienen als Leitfaden, anhand dessen Unternehmen die wichtigsten Praktiken in der Cybersicherheit identifizieren und priorisieren können. Die CISA CPG sollen einen Grundstandard definieren, um Herausforderungen bei der Cybersicherheit zu begegnen, denen Unternehmen sich täglich gegenübersehen. Sie dienen einem gemeinsamen Ziel, nämlich dem Fortschritt bei der Reduzierung von Cyberrisiken, um kritische Infrastrukturen wie Krankenhäuser, Energieversorgung, Transportsysteme und wichtige Produktionsanlagen zu schützen.

Mandiant unterstützt die CPG-Leitlinien der CISA als einen Anfang zur Risikominderung. Die CPG dienen als eine erste Etappe bei der Umsetzung des nationalen Sicherheitsmemorandums (NSM-5) der USA über die Verbesserung der Cybersicherheit von Steuerungssystemen kritischer Infrastrukturen („National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems"). Sie sind kein allumfassendes Cybersicherheitsprogramm, aber ein wichtiger erster Schritt auf dem Weg zu einer robusteren Cybersicherheitspraxis.

12. Mandiant, „INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems", 13. April 2022.
13. Cybersecurity and Infrastructure Security Agency, „CPG – Cross-Sector Cybersecurity Performance Goals", 2022.

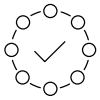
Die CPG sollen einen Mindeststandard zur Senkung von Cyberrisiken etablieren und nicht das endgültige Ziel darstellen. Wichtige Besonderheiten sind:

Zuordnung der Praktiken zu Teilaspekten der Cybersicherheit

Relevante Leitlinien speziell für IT und OT

Priorisierung der Praktiken zur Risikominderung

Praxisnähe durch Bezug auf von der CISA und ihren Partnern in der öffentlichen Verwaltung und Industrie beobachtete Bedrohungen



Anwendbarkeit über alle Sektoren kritischer Infrastrukturen hinweg

Die CPG nennen bestimmte Maßnahmen und Einrichtungen in Zusammenhang mit Betriebstechnologien (OT) und industriellen Steuerungssystemen (ICS), mit denen die entsprechenden Unternehmen den Schutz ihrer kritischen Infrastruktur verbessern können.

Unabhängig von der Größe eines Unternehmens erfordert der wirksame Schutz kritischer Infrastrukturen ein gutes Verständnis der relevanten Cyberbedrohungen, rigorose Sicherheitstests sowie eine unternehmensweite Bedrohungserkennung und -abwehr. Die CPG unterstützen Unternehmen bei ihren Überlegungen, wie sie mit ihren Investitionen innerhalb ihres Budgets, mit dem verfügbaren Personal und der vorhandenen Erfahrung eine möglichst große Schutzwirkung erreichen können. Die Investitionen zur Umsetzung der CPG werden „dazu beitragen, wirksam gegen ernsthafte Risiken für die Sicherheit, Gesundheit und Existenzgrundlage der amerikanischen Bevölkerung vorzugehen".[14]

14. Cybersecurity and Infrastructure Security Agency, „CPG – Cross-Sector Cybersecurity Performance Goals", 2022.

Verständnis relevanter Cyberbedrohungen

Die CPG leiten Unternehmen dazu an, das Bewusstsein für relevante Bedrohungen aufrechtzuerhalten und die Taktiken, Techniken und Prozesse (TTP) der Angreifer zu nutzen, um laufende Angriffe zu erkennen. Das Verständnis relevanter Cyberbedrohungen ist der Dreh- und Angelpunkt des Ansatzes von Mandiant für OT-Sicherheit: Wir leiten unsere Kunden dazu an, ihre Fähigkeiten zur Bedrohungserkennung sowohl in IT- als auch OT-Netzwerken durch umfassende Berücksichtigung der Situation auszubauen.[15] Wir sind davon überzeugt, dass Verteidiger und Incident-Response-Experten sich deutlich stärker den Eindringmethoden (d. h. den TTP) während des gesamten Angriffszyklus widmen sollten, von denen die meisten „Zwischensysteme", wie wir sie nennen, betreffen. Dabei handelt es sich überwiegend um Systeme, die die Netzwerkgrenzen von IT und OT überschreiten oder um jene vernetzten Workstations und Server innerhalb des OT-Netzwerks, deren Betriebssysteme und Protokolle den in der IT genutzten ähnlich oder gleich sind. Die Verengung des Fokus auf Eindringmethoden ist effektiv, da die Mehrzahl ausgereifter Angriffe auf die OT solche Zwischensysteme als Trittsteine zu ihrem eigentlichen Ziel nutzt.

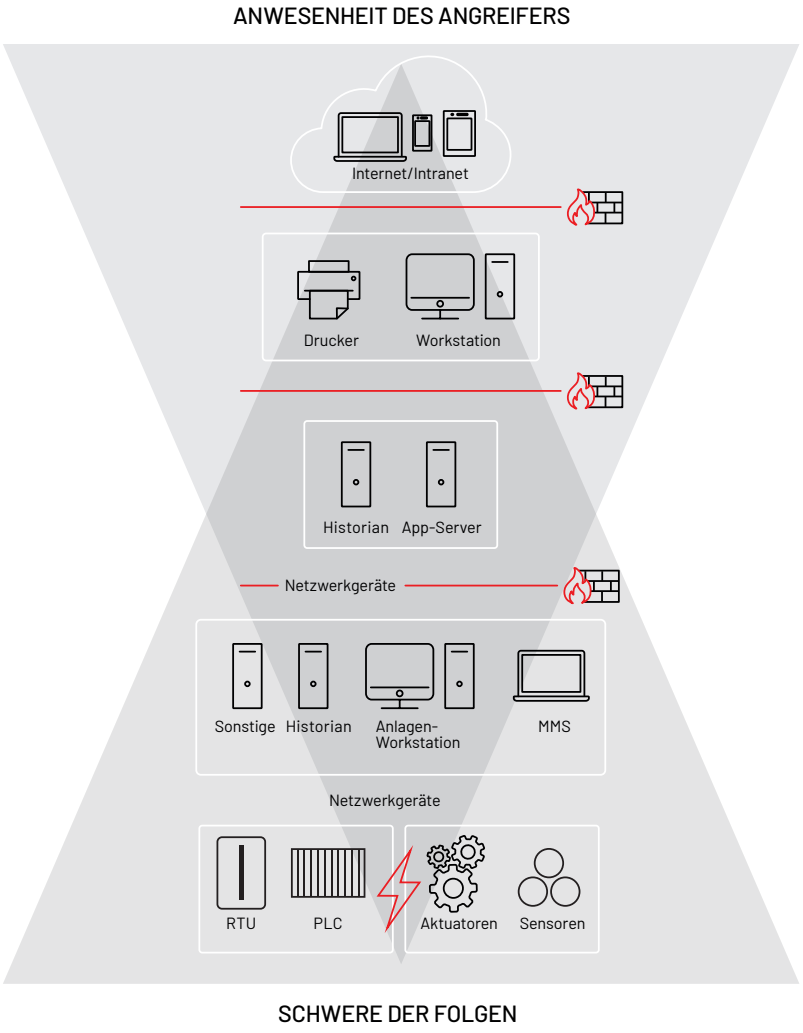


Abbildung 1: Der Trichter der Chancen zur Erkennung von OT-Bedrohungen

15. Mandiant, „The Mandiant Approach to Operational Technology Security", Dezember 2019.

Die größte Chance, einen gezielten Angriff auf die OT zu entdecken, besteht dort, wo die zwei Dreiecke in Abbildung 1 überlappen.[16] In diesem Bereich macht das Zusammenspiel der Anwesenheit des Angreifers und der Folgen seines Eindringens für den Betrieb die Erkennung von Bedrohungsaktivitäten durch die Sicherheitsteams einfacher und wirkungsvoller. Die Verteidiger müssen die Eindringmethoden der Angreifer verstehen und dieses Wissen für die Suche und Erkennung fortschrittlicher Bedrohungen nutzen. Die Bedrohungsjagd in der Nähe der DMZ und des Prozessleitsystems (PLS) der OT kann äußerst effizient sein, da die erkennbaren Kennzeichen des Eindringens immer noch vorhanden sind und die Schwere der möglichen Folgen des Eindringens hoch, aber immer noch nicht kritisch ist.

16. Mandiant, „The Mandiant Approach to Operational Technology Security", Dezember 2019.

2022

Im Jahr 2022 berichtete Mandiant darüber, dass bei erpresserischen Angriffen mit Ransomware vertrauliche OT- und Netzwerkdokumente erbeutet wurden.[17] Durch die Offenlegung sensibler OT-Daten durch Ransomware oder durch auf anderem Weg verursachte Datenlecks gelangen versierte Angreifer an Informationen über ihre Ziele, insbesondere über deren Infrastruktur, Anlagen, Sicherheitsschwachstellen und Prozesse. Mithilfe solcher Aufklärungsdaten entwickeln Angreifer wirkungsvollere und genauere Angriffe.

TABELLE 2: Als Folge von Ransomware-/Erpressungsangriffen preisgegebene Dokumente

Angaben zum Opfer	Erbeutete Inhalte
Hersteller von Industrie- und Personenzügen	Anmeldedaten für die Passwortadministration für ein OEM, Anforderungen an die Steuerungsarchitektur und Kommunikationskanäle für ein europäisches Straßenbahnfahrzeug, Backups von PLC-Projektdateien im TIA-Portal von Siemens und mehr
Zwei Öl- und Gasgesellschaften	Detaillierte Netzwerk- und Prozessdokumentation, einschließlich Diagramme, HMI, Kalkulationstabellen usw.
Integrator von Steuerungssystemen	Technische Dokumentation von Kundenprojekten (manche Dateien waren mit einem Passwort geschützt, was wir nicht zu knacken versuchten)
Wasserkrafterzeuger	Hauptsächlich Daten in Bezug auf Finanzen und Buchhaltung sowie eine Liste mit Namen, E-Mail-Adressen, Zugriffsrechten und einigen Passwörtern von Mitarbeitern aus IT, Anlagenwartung und Betrieb
Dienstleister für satellitengestütztes Tracking von Fahrzeugen	Produktdiagramme, grafische Darstellungen und Quellcode einer proprietären Plattform zur Verfolgung von Fahrzeugflotten über das globale Positionsbestimmungssystem (GPS)
Erzeuger von erneuerbarer Energie	Verträge zwischen dem Unternehmen und seinen Kunden über die Bedingungen für die Wartung und Bereitstellung von Infrastruktur für erneuerbare Energie, darunter die Vereinbarung, dass der Dienstleister über öffentliche Internet-IP-Adressen vollen Zugriff auf das SCADA-System des Drittanbieters erhält

- Setzen Sie gegenüber Mitarbeitern und Auftragnehmern, die auf Daten aus allen Netzwerksegmenten zugreifen können, robuste Richtlinien für den Umgang mit Daten durch, um sicherzustellen, dass Ihre internen Dokumente geschützt sind.
- Speichern Sie hochsensible Betriebsdaten nicht in Netzwerken mit einem niedrigeren Sicherheitsniveau.
- Achten Sie bei der Auswahl von Auftragnehmern besonders darauf, dass diese über umfassende Sicherheitsprogramme zum Schutz von Betriebsdaten verfügen.
- Falls Sie dennoch Opfer eines Ransomware-Angriffs werden, prüfen Sie genau den Wert sämtlicher offengelegter Daten, um zu bestimmen, welche Ausgleichsmaßnahmen die Erfolgsaussichten weiterer Eindringversuche verringern können.
- Wechseln Sie alle offengelegten Anmeldedaten und API-Schlüssel aus. Erwägen Sie den Austausch offengelegter IP-Adressen für wichtige Systeme und OT-Jump-Server.
- Führen Sie regelmäßig Red-Team-Übungen durch, um nach außen gedrungene und ungeschützte interne Daten zu identifizieren.

17. Mandiant, „1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information", Januar 2022.

Rigorose Sicherheitstests

Ein Schlüssel zur zuverlässigen Verbesserung des Sicherheitsstatus von OT-Netzwerken sind geschützte Tests der Sicherheitsmaßnahmen auf jeder Ebene des OT-Netzwerks hinsichtlich der häufigsten Angriffe und Malware-Familien, die auf kritische Anlagen abzielen. Die CISA CPG empfehlen Unternehmen, die Wirksamkeit und Abdeckung ihrer Cyberabwehr regelmäßig durch einen externen Anbieter überprüfen zu lassen.

Mandiant rät zu einem unternehmensspezifischen Programm, damit die Prüfungsanforderungen genau auf das jeweilige Unternehmen zugeschnitten sind. Ein umfassendes OT-Testprogramm ist am effektivsten, wenn es die Perspektive der Angreifer einnimmt, Simulation und Emulation nutzt, um die Auswirkungen auf den laufenden Betrieb zu minimieren, und eine geeignete Mischung von Red-Team-, Purple-Team- und Penetrationstests sowie Tests der Netzwerk- und Komponentensicherheit umfasst. Wenn proaktive Tests aufgrund der Anforderungen an die Betriebsbereitschaft von OT-Umgebungen in der Produktion nicht umsetzbar sind, empfiehlt Mandiant technische Beurteilungen, bei denen die Wirksamkeit von Netzwerksegmentierung, Zugangskontrollen, Netzwerküberwachungssystemen, Richtlinien zu vorübergehend angeschlossenen Geräten und Fähigkeiten für die Bedrohungsabwehr beurteilt werden. Durch kontinuierliche Tests wird nicht nur die Wirksamkeit von Sicherheitsmaßnahmen zu einem bestimmten Zeitpunkt beurteilt, sondern auch die Identifizierung komplexer Sicherheitsprobleme in integrierten Netzwerken (IT zu OT) ermöglicht, bevor sie von einem Angreifer ausgenutzt werden. Die laufende Validierung kann das unternehmenseigene Team auch auf die Überwachung der Umgebung und die Erkennung und Abwehr von Cybersicherheitsvorfällen vorbereiten. Unternehmen sollten an solche Programme die folgenden Erwartungen stellen: taktische Empfehlungen zur Begrenzung schwerwiegender festgestellter Probleme, strategische Empfehlungen zur langfristigen Verbesserung und die Identifizierung von mangelhaften Fähigkeiten der Mitarbeiter, die OT zu überwachen und auf Vorfälle angemessen zu reagieren.

Open-Platform-Communications-Server ermöglichen einen ähnlichen und herstellerunabhängigen Datenaustausch zwischen Maschinen, Geräten und Systemen in der industriellen Umgebung.

Bedrohungsabwehr und Wiederherstellung

In Abschnitt 7 legen die CISA CPG die Notwendigkeit dar, dass Unternehmen für relevante Bedrohungsszenarien Abwehrpläne für Cybersicherheitsvorfälle pflegen, üben und auf dem aktuellen Stand halten. Die Erfahrung von Mandiant an vorderster Front bei der Abwehr medienwirksamer Angriffe auf operative Technologie, wie TRITON und INCONTROLLER, hat zu einem tieferen Verständnis der Unterschiede bei der Bedrohungsabwehr bei IT und OT und der für die Abwehr von OT-Angriffen erforderlichen Tools und Vorgehensweisen geführt.

Die Ziele der Beseitigung und Eindämmung (d. h. die Entfernung der Bedrohung aus der Umgebung und die Wiederherstellung der Systeme zu normalen Betriebsbedingungen) sind zwar in beiden Fällen dieselben, aber die Tools können grundverschieden sein. Bei der Abwehr im IT-Bereich wird zur Untersuchung, Eindämmung und Wiederherstellung/Beseitigung routinemäßig Technologie zur Bedrohungserkennung und -abwehr am Endpunkt genutzt. Auf Servern oder Komponenten in OT-Netzwerken sind diese Tools typischerweise nicht installiert.

Die Eindämmung ist in der IT relativ einfach und hat oft deutlich weniger „Nebenwirkungen", als dies in komplexen OT-Umgebungen der Fall sein kann. Zum Beispiel ist das Anhalten und Starten bestimmter Funktionen oder auch das Entfernen eines ganzen Systems im IT-Netzwerk gängige Praxis. Solche Maßnahmen können weiter reichende Folgen haben, wenn sie an einer OT-Komponente vorgenommen werden. Damit Prozesse gestartet oder angehalten oder Komponenten offline geschaltet werden können, ohne den Betrieb zu beeinträchtigen, ist ein umfassendes Verständnis der zugrunde liegenden Prozesse vonnöten. Anderenfalls könnte es zu erheblichen Ausfallzeiten oder möglicherweise sogar Risiken für Leib und Leben kommen. Werden zum Beispiel OPC-Server (Open Platform Communications) unüberlegt abgeschaltet, kann dies für Wochen die gesamte Fertigungslinie stören. Eine detaillierte Planung außerhalb einer laufenden Bedrohungsabwehr gibt Systemeignern eine Grundlage für risikobasierte Entscheidungen anhand möglicher Ausfallzeiten, Produktionsverluste oder lebensbedrohlicher Risiken. Ist das Unternehmen in der Lage, die Ziele und Motive potenzieller Angreifer zu verstehen, kann dies den Systemeigner dabei unterstützen, sicherere, weniger risikobehaftete Entscheidungen zu treffen.

Nicht zuletzt bestehen OT-Netzwerke aus vielen herstellergesteuerten Teilnetzwerken, auf die das Unternehmen selbst keinen direkten Zugriff hat. Mandiant empfiehlt die Erstellung von Abwehrplänen und Leitfäden, die Drittsysteme einbeziehen und gemeinsam mit den jeweiligen Herstellern getestet werden. Die Wichtigkeit, einen Plan zur schnellen, effizienten und angemessenen Behebung von Cybersicherheitsvorfällen zu haben und sich daran zu halten, kann nicht überbetont werden.

Mandiant entwickelt seine Angebote für OT-Sicherheit anhand der „fünf Funktionen" des Cybersicherheits-Frameworks des NIST[18], zu dem die CISA CPG eine Ergänzung sind, und passt seine Services an den Lebenszyklus des Cybersicherheitsrisikomanagements des Unternehmens an.

18. NIST, „Cybersecurity Framework, The Five Functions", Mai 2021.

		Identifizieren	Schützen	Erkennen	Abwehren	Wieder-herstellen
Bedrohungs-daten	Threat Intelligence als Abonnement	■	■	■		
	Dedizierter Security-Analyst	■	■	■		
	Schwachstellenanalysen	■	■			
	Kundenspezifische Analyse und Blackbox-Beurteilung	■				
Beratung	Gesundheitscheck	■	■	■		
	Bewertung von Sicherheitsprogrammen	■	■			
	Angriffs- und Penetrationstests	■	■	■		
	Incident-Response-Planung	■			■	■
	Incident Response				■	■
	Sicherheitsschulungen	■	■			
	Dedizierter Berater	■	■	■	■	■
Managed Defense für OT	Jumpstart	■	■			
	Laufende Überwachung		■	■	■	
Technologie von Dritt-anbietern	Überwachung des OT-Netzwerkprotokolls	■		■		

Abbildung 2: OT-spezifische Angebote von Mandiant

Mandiant bietet aus erster Hand gewonnene Erkenntnisse zur Cybersicherheit, gepaart mit einem tiefgreifenden Wissen über die Funktionsweise industrieller Steuerungssysteme aus jahrzehntelanger praktischer Erfahrung aus Einsätzen in ICS- und OT-Umgebungen. Die OT-Experten von Mandiant führen ausgefeilte Sicherheitstests durch, um Industrieunternehmen dabei zu unterstützen, ihre Fähigkeiten zur Erkennung und Begrenzung von Angriffen über ganze OT-Netzwerke hinweg zu verbessern. Nehmen auch Sie unsere Unterstützung bei der Umsetzung der CISA CPG in Anspruch – für mehr Sicherheit in der OT-Umgebung und eine Stärkung Ihrer Fähigkeiten zur Bedrohungsabwehr.

Zusammenfassung

Diese Ausgabe von „Der Vorteil des Verteidigers – Eine Momentaufnahme der Cybersicherheitslage“ wendet sich an Unternehmen, die die Umstellung von herkömmlichen Passwörtern und Mehrfaktor-Authentifizierung (MFA) auf eine passwortlose Authentifizierung planen. Unsere Empfehlung ist es, für die Authentifizierung am Backend und den Zugriff auf alle Geräte und Anwendungen starke MFA-Methoden auszubauen und Single-Sign-on-Lösungen von Drittanbietern in Erwägung zu ziehen. Denjenigen, die sich auf dem unbeständigen Markt für Cyberversicherungen zurechtfinden müssen, geben wir den Rat, im Vorfeld des Vertragsabschlusses Rechtsberatung und Risikomanagement einzubeziehen, die Musterpolice sorgfältig zu prüfen und ihren Versicherungsanbieter als Partner beim allgemeinen Risikomanagement zu betrachten.

Außerdem zeigen wir in dieser Ausgabe, wie die in „Der Vorteil des Verteidigers“ dargelegten sechs wichtigen Funktionen der Cyberabwehr den Cross-Sector Cybersecurity Performance Goals (CPG) entsprechen, die die U.S. Cybersecurity and Infrastructure Agency (CISA) im letzten Jahr veröffentlicht hat. Dabei handelt es sich um Cybersicherheitspraktiken, die Eigentümer und Betreiber kritischer Infrastrukturen umsetzen können, um Risiken maßgeblich zu senken. In einer Fallstudie präsentieren wir die Taktiken eines optimierten SOC bei der Untersuchung eines Angriffs auf eine Lieferkette. Die Analysten untersuchen relevante Warnmeldungen in einem zusammenhängenden Einsatz, bei dem ihr Training, ihre Erfahrung und ihr kritisches Denken entscheidende Faktoren sind.

Wissen ist Macht – das gilt auch im Kampf gegen Cyberkriminelle. Mit unserem Bericht „Der Vorteil des Verteidigers – Eine Momentaufnahme der Cybersicherheitslage“ möchten wir einen Beitrag dazu leisten und mithilfe relevanter Informationen und Daten Sicherheitsteams und Führungskräfte befähigen, fundierte Entscheidungen zu treffen. Die Cybersicherheitsbranche muss eng zusammenarbeiten und Informationen austauschen, damit Incident-Response-Teams eine Chance haben. „Der Vorteil des Verteidigers – Eine Momentaufnahme der Cybersicherheitslage“ ist nur ein Beitrag von Mandiant zu diesen Bemühungen.

Weitere Informationen finden Sie unter www.mandiant.de

Mandiant

11951 Freedom Dr, 6th Fl, Reston,
Virginia 20190, USA
+1 703 935 8012
+1 833 3MANDIANT (362 6342)
info@mandiant.com

Über Mandiant

Mandiant ist als führender Anbieter von dynamischen Cyberabwehrlösungen, Threat Intelligence und Incident-Response-Services bekannt. Mandiant nutzt seine jahrzehntelange Praxiserfahrung, um Unternehmen und Institutionen bei der souveränen Prävention und Abwehr von Cyberbedrohungen zu unterstützen. Mandiant gehört nun zu Google Cloud.

MANDIANT
NOW PART OF Google Cloud