Februar 2026

Bedrohungsbericht

Der Managed XDR Global Threat Report

Wie Angreifer Organisationen und Security-Lücken ins Visier nehmen

Barracuda®
Your business, secured.

Inhalt

Einleitung 3

Wichtige Erkenntnisse 4

Wie Angreifer Organisationen angreifen 5

Wie Organisationen sich angreifbar machen 10

Die anhaltende Bedrohung durch Ransomware 18

Fazit: Wie man in einer Welt komplexer Bedrohungen sicher bleibt 21

Einleitung

Die fortschrittlichen Tools und Experten von Barracuda Managed XDR überwachen und schützen die Netzwerke der Kunden rund um die Uhr, 365 Tage im Jahr. Jede Minute erkennt die Lösung eine Security-Warnung und reagiert darauf. Alle 15 Minuten sendet es eine Warnung an einen Kunden, und alle 60 Minuten blockiert es automatisch eine hochgradige Bedrohung, wie z. B. ein kompromittiertes Gerät oder einen sich entwickelnden Ransomware-Vorfall.

Wird ein einzelnes Warnsignal nicht behoben, kann es sich schnell zu einem weitreichenden Vorfall ausweiten, der den Geschäftsbetrieb stört, die Produktivität mindert, sensible Daten gefährdet und die finanzielle Stabilität sowie den Ruf der Marke schädigt. Keine Organisation ist immun; Angreifer zielen auf Unternehmen jeder Größe, aus allen Branchen und Regionen ab.

Viele Faktoren können Ziele angreifbar machen — Security-Lücken, manipulierte Geräte, ungepatchte Systeme, Versäumnisse, Fehlkonfigurationen — und es mangelt an Zeit und Ressourcen, um den Eindringling zu erkennen, die Angreifer zu entfernen und die Tür hinter ihnen fest zu verschließen.

Dieser Bericht soll IT- und Security-Fachleuten in ressourcenbeschränkten Organisationen dabei helfen, besser zu verstehen, wie Angreifer potenzielle Opfer ins Visier nehmen und welche Security-Lücken sie auszunutzen versuchen. Wir liefern Beispiele für reale Vorfälle und Empfehlungen, wie Sie sicher und cyberresilient bleiben können.

In einer Welt zunehmend komplexer und schwer fassbarer Cyberbedrohungen stehen Organisationen nicht allein vor der Herausforderung. Ihr Sicherheitsanbieter verfügt über die Werkzeuge und Einblicke, um Ihnen bei der Lösung der in diesem Bericht identifizierten Probleme zu helfen — und wir stehen Ihnen bei jedem Schritt zur Seite.

Die zugrundeliegenden Daten

Die in diesem Bericht detaillierten Ergebnisse basieren auf Barracuda Managed XDR dem einzigartigenDatensatz mit mehr als zwei Billionen IT-Ereignissen, die im Jahr 2025 gesammelt wurden, fast 600.000 Securitywarnungen und mehr als 300.000 geschützten Endpunkten, Firewalls, Servern, Cloud-Assets und mehr. Rund 53.000 hochschwere Bedrohungen wurden von BARRACUDA Managed XDRs Securityorchestrierungs- und automatisierten Reaktionsplattform (SOAR) triagiert.

Zentrale Ergebnisse

100 %

der Sicherheitsvorfälle beinhaltete mindestens einen ungeschützten oder unbefugten Endpunkt

96 %

der Vorfälle beinhaltete laterale Bewegungen, die mit der Freisetzung von Ransomware endeten

66 %

der Vorfälle betrafen die Lieferkette oder Dritte (gegenüber 45 % im Jahr 2024)

3 Stunden

der schnellste Ransomware-Angriff, vom Eindringen bis zur Verschlüsselung

90 %

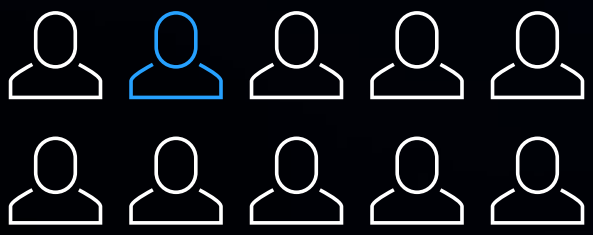
der Ransomware-Vorfällen nutzen Firewalls aus

13 Jahre

die am häufigsten entdeckte Schwachstelle ist ein Fehler aus dem Jahr 2013 in einer veralteten Verschlüsselung

1 von 10

entdeckte Schwachstellen haben eine bekannte Ausnutzung



Wie Angreifer Organisationen ins Visier nehmen

Effektive Extended Detection and Response-(XDR-)Lösungen sind darauf ausgelegt, eingehende Bedrohungen im frühesten Stadium der Angriffskette abzufangen — dem Punkt der anfänglichen Kompromittierung und des Zugriffs. Barracuda Managed XDR bildet da keine Ausnahme. Es bietet zudem eine bessere Übersicht über spätere Angriffsphasen, einschließlich seitlicher Bewegungen und Einschläge. Diese breite Fähigkeit spiegelt sich im Inhalt dieses Berichts wider.

An der Spitze der Liste der am häufigsten erkannten Bedrohungen gegen Organisationen in den letzten 12 Monaten stehen Angriffe, die auf Identitäten und die Sicherheit von Identitäten abzielen.

Dazu gehören ungewöhnliche oder unerwartete Anmeldungen zu einem Nutzerkonto. Dies sind Verbindungen, die nicht dem typischen Verhaltensmuster des Nutzers in Bezug auf Gerät, Ort oder Zeit entsprechen. Solche Erkennungen sind ein starker Indikator für den Diebstahl von Zugangsdaten und die Kompromittierung von Konten. Weitere Warnsignale sind Verbindungsversuche von einem gesperrten Standort sowie die Regel der „unmöglichen Reise“, bei der sich ein Nutzer von einem zweiten Standort einloggt, den er in der Zeit zwischen den Logins unmöglich hätte erreichen können.

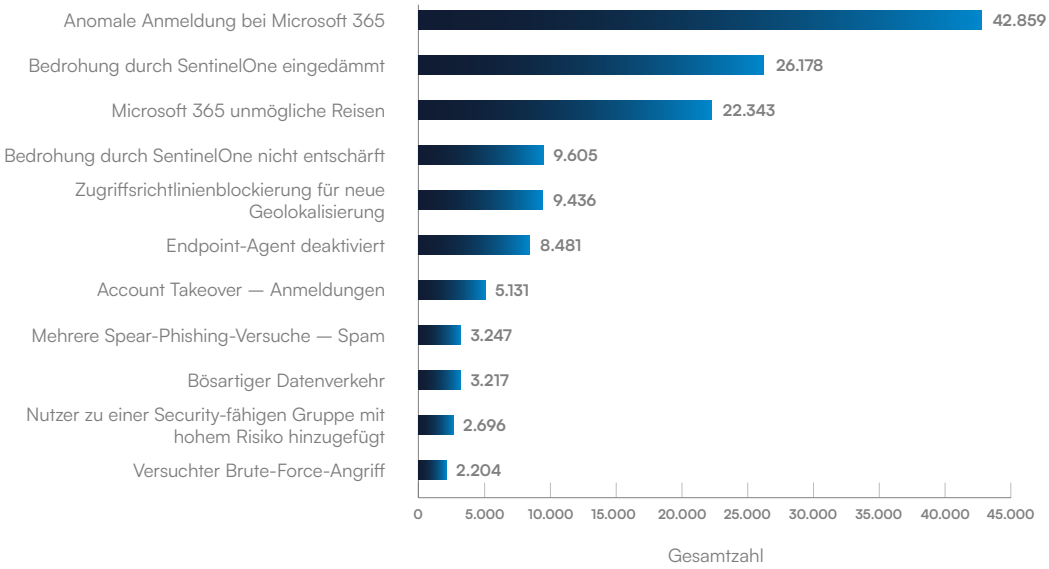


ABBILDUNG 1

Top-Angriffs-Entdeckungengegen Organisationen

Die Liste der wichtigsten Erkennungen umfasst auch Aktivitäten, die darauf hindeuten könnten, dass ein Konto kompromittiert wurde und Angreifer im Netzwerk sind. Security-Teams müssen solche Erkennungen sofort untersuchen. Sie umfassen Anzeichen, die darauf hindeuten, dass jemand versucht hat, den Endpunktschutz zu umgehen oder zu deaktivieren, sowie Benachrichtigungen, dass ein Nutzer zu einer sicherheitssensiblen Gruppe hinzugefügt wurde, was ein Angreifer sein könnte, der versucht, seine Berechtigungen zu eskalieren.

Wie Angreifer nach dem Eindringen in das System die Berechtigungen manipulieren

Die Eskalation von Privilegien ist für Angreifer entscheidend, da sie begrenzten Zugriff in vollständige administrative Kontrolle verwandelt, was es ihnen ermöglicht, Verteidigungen zu deaktivieren, sich seitlich zwischen Systemen zu bewegen und auf sensible Daten zuzugreifen. Das Ergebnis kann ein groß angelegter Kompromiss und die Freisetzung von Ransomware sein.

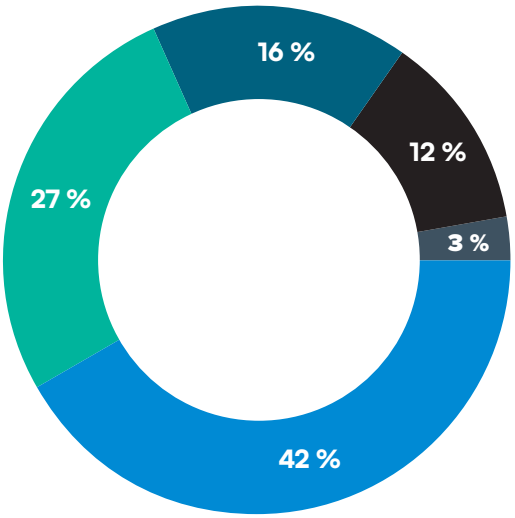


ABBILDUNG 2

Wie Angreifer privilegierte Rechte manipulieren

- Windows — Ein Nutzer wurde einer Gruppe mit Hochrisiko-Sicherheitsrechten hinzugefügt
- Windows — Ein Nutzer wurde aus einer Gruppe mit Hochrisiko-Sicherheitsrechten entfernt
- Microsoft 365 — Ein Nutzer wurde als globaler Administrator hinzugefügt
- Microsoft 365 — Ein Nutzer wurde als globaler Administrator entfernt
- FortiGate Firewall — Ein Nutzer wurde als Administrator hinzugefügt

Die Firewall, Windows- und Microsoft-365-Security-Tools von Barracuda Managed XDR haben die folgenden Verhaltensweisen erkannt, die auf eine versuchte Privilegien-Eskalation hinweisen:

Windows — hat einen Nutzer zu einer Gruppe mit Hochrisiko-Sicherheitsrechten hinzugefügt (was 42 % der verdächtigen Privilegien-Eskalationen ausmacht)

- **Das bedeutet:** Ein Nutzer wurde einer Gruppe mit weitreichenden Berechtigungen hinzugefügt (z. B. Domänenadministratoren).
- **Angreifer können es nutzen, um:** Sich lateral zu bewegen, Malware zu installieren oder Daten zu exfiltrieren.
- **So bleiben Sie sicher:** Überwachen Sie Gruppenänderungen und verwalten Sie die Zuweisung aller privilegierten Zugriffsrechte.

Windows — ein Nutzer wurde aus einer Gruppe mit Hochrisiko-Sicherheitsrechten entfernt (27 %)

- **Das bedeutet:** Ein Nutzer wurde aus einer Gruppe mit hohen Privilegien entfernt.
- **Angreifer können es nutzen, um:** Ihre Spuren nach einer Privilegien-Eskalation zu verwischen.
- **So bleiben Sie sicher:** Untersuchen Sie, warum die Löschung erfolgt ist, und prüfen Sie, ob vor der Löschung ein Missbrauch stattgefunden hat.

Microsoft 365 — Ein Nutzer wurde als globaler Administrator hinzugefügt (16%)

- **Das bedeutet:** Jemandem wurde die höchste Zugriffsebene in Microsoft 365 gewährt.
- **Angreifer können es nutzen, um:** Neue Konten zu erstellen, Daten zu stehlen oder die Security zu deaktivieren.
- **So bleiben Sie sicher:** Überprüfen Sie Änderungen der Administratorrolle, setzen Sie die Multi-Faktor-Authentifizierung (MFA) durch und führen Sie geeignete Überprüfungs- und Genehmigungsprozesse ein.

Microsoft 365 — Ein Nutzer wurde als globaler Administrator entfernt (12%)

- **Das bedeutet:** Jemand hat seine globalen Administratorrechte verloren.
- **Angreifer können es nutzen, um:** Die Erkennung zu umgehen, indem sie ihre hinzugefügten Konten entfernen.
- **So bleiben Sie sicher:** Überprüfen Sie, ob die Änderung autorisiert wurde, und prüfen Sie die Audit-Protokolle auf verdächtige Aktivitäten oder Missbrauch.

FortiGate-Firewall — Ein Nutzer wurde als Administrator für die Firewall hinzugefügt (3 %)

- **Das bedeutet:** Ein neues Administratorkonto wurde auf der Firewall erstellt.
- **Angreifer können es nutzen, um:** Schutzmaßnahmen zu deaktivieren und Hintertüren zu öffnen.
- **So bleiben Sie sicher:** Bestätigen Sie die Kontolegitimität und setzen Sie strenge Administratorkontrollen durch.

Vorfallbericht — Der bösartige Anhang, der zu einem RAT führte

Ein Remote Access Trojan (RAT) wurde auf den Systemen eines Kunden gefunden, nachdem ein Mitarbeiter versehentlich eine bösartige ausführbare Datei heruntergeladen hatte. Die Datei versuchte sofort, Persistenz zu etablieren: Sie bat darum, sich als Windows-Dienst zu registrieren, was es ihr ermöglichen würde, automatisch zu starten, im Hintergrund zu laufen und mit systemweiten Zugriffsrechten zu operieren, sodass sie das System ohne Unterstützung aus der Ferne steuern konnte. Es wurde auch versucht, das vertrauenswürdige Fernmanagement-Tool ScreenConnect über PowerShell zu installieren.

Versteckt sich vor aller Augen

Das Hinzufügen und Entfernen von Nutzern aus privilegierten Zugriffsgruppen ist eine legitime IT-Aktivität. Die Fähigkeit von Angreifern, bösartiges Verhalten unter normalen, alltäglichen Aufgaben und Tools zu verstecken, ist eine der größten Herausforderungen, vor denen Security-Teams heute stehen.

Dieser Ansatz des „living off the land" (LOTL) ist auf dem Vormarsch. Hierbei nutzen Bedrohungsakteure legitime Software-Tools und -Techniken, um einer Entdeckung zu entgehen. Glücklicherweise hilft KI fortschrittlichen Security-Systemen dabei, subtile Anomalien in scheinbar harmlosen Aktivitäten zu erkennen, die untersucht und abgemildert werden können.

Vorfallbericht — Akira-Ransomware missbraucht das Fernverwaltungstool des Opfers gegen sich selbst

Die Angreifer verschafften sich Zugang zum Domain Controller (DC) und installierten Datto RMM. Ihr Vorgehen ähnelte weitgehend dem, was ein Backup-Agent im Rahmen geplanter Aufträge rechtmäßig tun würde, sodass alles wie normale IT-Aktivitäten aussah.

Ein Wort zu Tools für Fernzugriff und Management (RMM)

Fernzugriffstools werden zunehmend zum Ziel von Angreifern. Wenn es gelingt, ein RMM-Tool zu kompromittieren, erhalten Angreifer eine erhebliche Machtfülle und verringern gleichzeitig das Risiko, entdeckt zu werden, da RMMs in Unternehmen weit verbreitet sind.

In den letzten 12 Monaten hat Barracuda Managed XDR-Vorfälle gemildert, die unter anderem den Missbrauch von SonicWall SSL-VPN (einem beliebten virtuellen privaten Netzwerk), ScreenConnect, RDP (Remote Desktop Protocol), PsExec (ein Kommandozeilen-Tool zum Ausführen von Programmen und Befehlen auf entfernten Computern), AnyDesk und anderen Firewall-VPNs umfassten.

Um das Risiko zu verringern, müssen Sicherheitsteams Erkennungssysteme einsetzen, die gezielt auf den Missbrauch von RMM achten. Zum Beispiel hat Barracuda Managed XDR eine Erkennungsregel entwickelt, die Telemetrie von Endpunkten nutzt, um Anfragen zu identifizieren, die von ScreenConnect an verdächtige Top-Level-Domains (TLDs) gesendet werden.

Rote-Flagge-Kombinationen

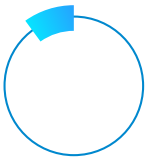
Verdächtige Aktivitäten können auch durch einen Blick auf das Gesamtbild erkannt werden. Eine Analyse realer Vorfälle mit Barracuda Managed XDR in den letzten 12 Monaten identifizierte die folgenden häufigen Kombinationen von Tools/Techniken und Verhaltensweisen:

66 %

der Fälle beinhalteten dateilose Malware, die PowerShell als primäre Ausführungsmethode verwendete. PowerShell ist ein plattformunabhängiges Werkzeug, das zur Automatisierung von Aufgaben und zur Verwaltung von Konfigurationen verwendet wird.

44 %

der Vorfälle im Zusammenhang mit Firewalls betrafen Passwort-Spraying — bei dem Angreifer viele gängige Passwörter mit gestohlenen Benutzernamen ausprobierten.



10 %

der Server-Security-Verletzungen beinhalteten das Löschen von Aktivitätsprotokollen, um die Spuren der Angreifer zu verwischen.

96 %

der Fälle beinhaltete laterale Bewegungen, die zum Einsatz von Ransomware führten.

90 %

der Ransomware-Angriffe nutzten Firewalls über eine CVE (eine klassifizierte Software-Schwachstelle) oder ein anfälliges Konto aus.

34 %

der Vorfälle betrafen Social Engineering, bei dem Nutzer dazu verleitet wurden, potenziell bösartige Dateien herunterzuladen.

Damit Angriffe erfolgreich sind, müssen Angreifer Lücken in der Security ihrer Opfer finden und ausnutzen. Die Detektionsdaten und Zwischenfalleinblicke von Barracuda Managed XDR werfen ein Licht auf einige der potenziellen Schwachstellen, die Ziele im letzten Jahr anfällig für Cyberbedrohungen gemacht haben.

Wie Unternehmen sich selbst exponieren

Die größten Schwachstellen der Netzwerk-Security

Unzureichende oder veraltete Verschlüsselungsmethoden, die sensiblen Datenverkehr nicht schützen, sowie das Fehlen einer ordnungsgemäßen Validierung — oder Zertifizierung — der Netzwerkaktivitäten können von Angreifern genutzt werden, um ihre Angriffe weiter zu verstärken.

Barracuda Managed XDR hat im vergangenen Jahr die folgenden Netzwerk-Security-Risiken identifiziert:

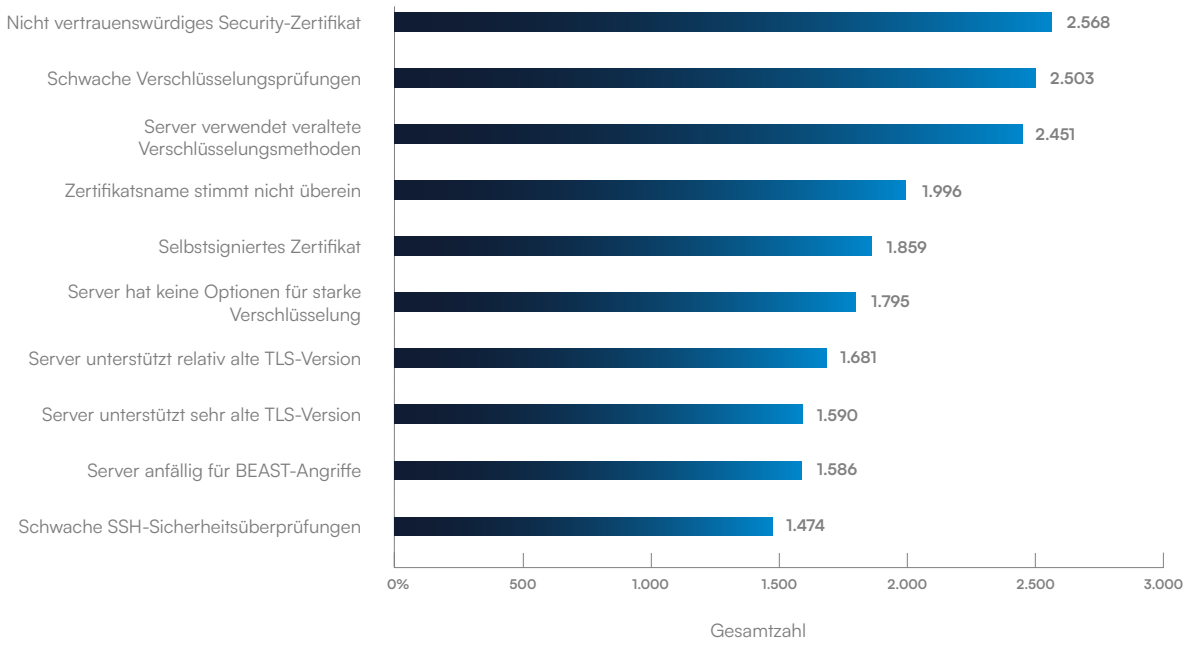


ABBILDUNG 3

Die größten Schwachstellen der Netzwerk-Security

Nicht vertrauenswürdiges Sicherheitszertifikat

Was das bedeutet:

Das vom Server vorgelegte Zertifikat wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt.

Angreifer können es nutzen, um:

Sich als legitime Website auszugeben und sich so in die legitime Kommunikation einzuklinken, um Daten zu stehlen, Security zu umgehen, bösartige Inhalte einzuschleusen und vieles mehr.

So bleiben Sie sicher:

Verwenden Sie Zertifikate von renommierten Zertifizierungsstellen.

Für technischere Teams: Implementieren Sie eine ordnungsgemäße Zertifikatsvalidierung und aktivieren Sie das „Zertifikats-Pinning“ (bei dem die Anwendung nur einem bestimmten Zertifikat vertraut, wenn sie sich mit einem Server verbindet). Es ist auch wichtig zu überprüfen, ob das Zertifikat einer Anwendung widerrufen wurde (mit Tools wie CRL und OCSP), um das Vertrauen in kompromittierte Zertifikate zu vermeiden. Siehe: OWASP-Zertifikatsvalidierung.

Schwache Verschlüsselungsprüfungen

Was das bedeutet:

Der Server verwendet schwache Algorithmen oder unzureichende Schlüssellängen für die Verschlüsselung.

Angreifer können es nutzen, um:

Durch Brute-Force-Angriffe oder das Ausnutzen von Sicherheitslücken sensible Daten wie Passwörter und Finanzinformationen zu entschlüsseln. Beim Brute-Forcing werden viele verschiedene Kombinationen von Benutzername und Passwort ausprobiert, um zu sehen, ob eine davon funktioniert.

So bleiben Sie sicher:

Setzen Sie starke Verschlüsselungsstandards wie AES-256, RSA-2048+ durch.

Für technischere Teams: Deaktivieren Sie schwache Verschlüsselungen und überprüfen Sie regelmäßig die Konfigurationen. Erwägen Sie die Implementierung von Elliptic Curve Cryptography (ECC), wie ECDSA oder ECDHE, um die Sicherheit und Leistung zu verbessern (siehe: NIST ECC-Empfehlungen). Verwenden Sie Perfect Forward Secrecy-(PFS-)Chiffriersuiten, um vergangene Sitzungen zu schützen, falls die Schlüssel kompromittiert werden.

Server verwendet veraltete Verschlüsselungsmethoden

Was das bedeutet:

Der Server stützt sich auf ausgemusterte Algorithmen wie MD5, SHA-1 oder RC4.

Angreifer können es nutzen, um:

Bekannte Schwachstellen auszunutzen, um Verschlüsselung zu knacken oder Signaturen zu fälschen, was zu Datenpannen führt.

So bleiben Sie sicher:

Aktualisieren Sie auf moderne Algorithmen wie SHA-256 oder AES und folgen Sie branchenüblichen Best Practices (z. B. den oben genannten NIST-Richtlinien).

Für technischere Teams: Entfernen Sie die Unterstützung für veraltete Algorithmen (MD5, SHA-1, RC4) aus allen Konfigurationen. Testen Sie mit Tools wie SSL Labs, um zu überprüfen, dass keine veralteten Algorithmen aktiviert sind. Siehe: SSL-Labs-Test.

Zertifikatsname stimmt nicht überein

Was das bedeutet:

Der Domänenname stimmt nicht mit dem Common Name (CN) oder dem Subject Alternative Name (SAN) des Zertifikats überein.

Angreifer können es nutzen, um:

Abfangangriffe zu starten, indem Sie den Datenverkehr auf einen bösartigen Server umleiten.

So bleiben Sie sicher:

Stellen Sie sicher, dass die Zertifikate mit allen verwendeten Domänen/Unterdomänen übereinstimmen.

Für technischere Teams: Verwenden Sie SAN-Felder für Multi-Domain-Zertifikate. Automatisieren Sie das Zertifikats-Management, um Fehlübereinstimmungen bei Erneuerungen zu vermeiden.

Selbstsigniertes Zertifikat

Was das bedeutet:

Das Zertifikat wird von der gleichen Einheit signiert, die es besitzt, und nicht von einer vertrauenswürdigen Zertifizierungsstelle.

Angreifer können es nutzen, um:

Es einfacher zu machen, Server zu imitieren, da jeder selbstsignierte Zertifikate erstellen kann.

So bleiben Sie sicher:

Verwenden Sie von Zertifizierungsstellen ausgestellte Zertifikate für öffentliche Dienste und beschränken Sie selbstsignierte Zertifikate auf interne Systeme.

Für technischere Teams: Pflegen Sie eine private Zertifizierungsstelle für die interne Nutzung und verteilen Sie deren Root-Zertifikat sicher. Achten Sie auf unautorisierte, selbstsignierte Zertifikate in Ihrem Netzwerk.

Dem Server fehlen starke Verschlüsselungsoptionen

Was das bedeutet:

Der Server bietet keine modernen, sicheren Verschlüsselungssuiten an.

Angreifer können es nutzen, um:

Ein Downgrade auf eine schwächere Verschlüsselung zu erzwingen.

So bleiben Sie sicher:

Konfigurieren Sie die Server so, dass sie starke Verschlüsselungssuiten unterstützen, wie z. B. Transport Layer Security (TLS 1.2/1.3) mit AES-GCM.

Für technischere Teams: Deaktivieren Sie die Unterstützung für schwache oder unsichere TLS-Chiffreoptionen wie NULL oder EXPORT, sodass nur starke, verschlüsselte und authentifizierte Verbindungen erlaubt sind. Aktualisieren Sie regelmäßig die Serversoftware, um die neuesten Protokolle und Chiffresuiten zu unterstützen.

Server unterstützt ältere Versionen von TLS

Was das bedeutet:

Die verwendete TLS-Version ist veraltet und anfällig für Angriffe.

Angreifer können es nutzen, um:

Protokollschwachstellen für Interception- oder Downgrade-Angriffe auszunutzen, die das System dazu verleiten, ein älteres, schwächeres Sicherheitsprotokoll zu verwenden.

So bleiben Sie sicher:

Aktualisieren Sie die verwendete TLS-Version.

Für technischere Teams: Deaktivieren Sie TLS 1.0 und 1.1. Unterstützt nur TLS 1.2 und 1.3. Siehe: Mozilla-TLS-Empfehlungen.

Server unterstützt sehr alte TLS-Version

Was das bedeutet:

Die verwendete TLS-Version ist veraltet und unsicher.

Angreifer können es nutzen, um:

Bekannte Schwachstellen auszunutzen.

So bleiben Sie sicher:

Aktualisieren Sie die verwendete TLS-Version.

Für technischere Teams: Entfernen Sie SSLv2, SSLv3 und frühe TLS-Versionen vollständig. Verwenden Sie automatisierte Tools, um nach Unterstützung für Legacy-Protokolle zu suchen.

Server anfällig für BEAST-Angriff

Was das bedeutet:

BEAST-Angriffe (Browser Exploit Against SSL/TLS) zielen auf ältere Versionen von TLS ab, die Schwächen in ihrer blockbasierten Verschlüsselung aufweisen.

Angreifer können es nutzen, um:

HTTPS (Hypertext Transfer Protocol Secure) entschlüsseln — eine sichere Version des grundlegenden Web-Kommunikationsprotokolls) kann Verkehr und vertrauliche Daten offenlegen.

So bleiben Sie sicher:

Aktualisieren Sie auf die neueste Version von TLS und verwenden Sie sichere Verschlüsselungssammlungen.

Für technischere Teams: Erwägen Sie TLS 1.2+ mit den Verschlüsselungssuiten AES-GCM oder ChaCha20-Poly1305. Deaktivieren Sie CBC-Modus-Verschlüsselungen in älteren TLS-Versionen.

Schwache SSH-Sicherheitsüberprüfungen

Was das bedeutet:

Die SSH-Konfiguration verwendet schwache Algorithmen oder veraltete Protokolle. SSH (Secure Shell) ist ein sicheres Netzwerkprotokoll, das für den Fernzugriff und die Fernsteuerung von Computern über ein ungesichertes Netzwerk wie das Internet verwendet wird.

Angreifer können es nutzen, um:

Durch Brute-Force-Angriffe auf Zugangsdaten oder Ausnutzen schwacher Schlüssel unbefugten Zugriff zu erlangen.

So bleiben Sie sicher:

Setzen Sie auf starke Schlüsselaustauschalgorithmen, deaktivieren Sie schwache SSH-Protokolle, verwenden Sie schlüsselbasierte Authentifizierung und implementieren Sie spezielle Intrusion-Prevention-Tools, die Server vor Brute-Force-Angriffen schützen, wie z. B. Fail2Ban oder ähnliche.

Für technisch Teams: Verwenden Sie nur SSH-Protokoll Version 2. Setzen Sie Mindestschlüssellängen durch (z. B. RSA 4096, Ed25519). Deaktivieren Sie, wenn möglich, die Passwortauthentifizierung und verwenden Sie die schlüsselbasierte Authentifizierung. Beschränken Sie den SSH-Zugriff per IP und verwenden Sie Firewallregeln. Aktualisieren Sie regelmäßig die SSH-Serversoftware. Siehe: SSH-Security-Best-Practices.

Die am häufigsten erkannten CVE-Software-Schwachstellen

Veraltete und ungepatchte Software ist ein Magnet für Cyberbedrohungen. Laut Barracuda Managed Vulnerability Security, sind dies die wichtigsten Software-Schwachstellen, die in den letzten Jahren in Kundennetzwerken identifiziert wurden:

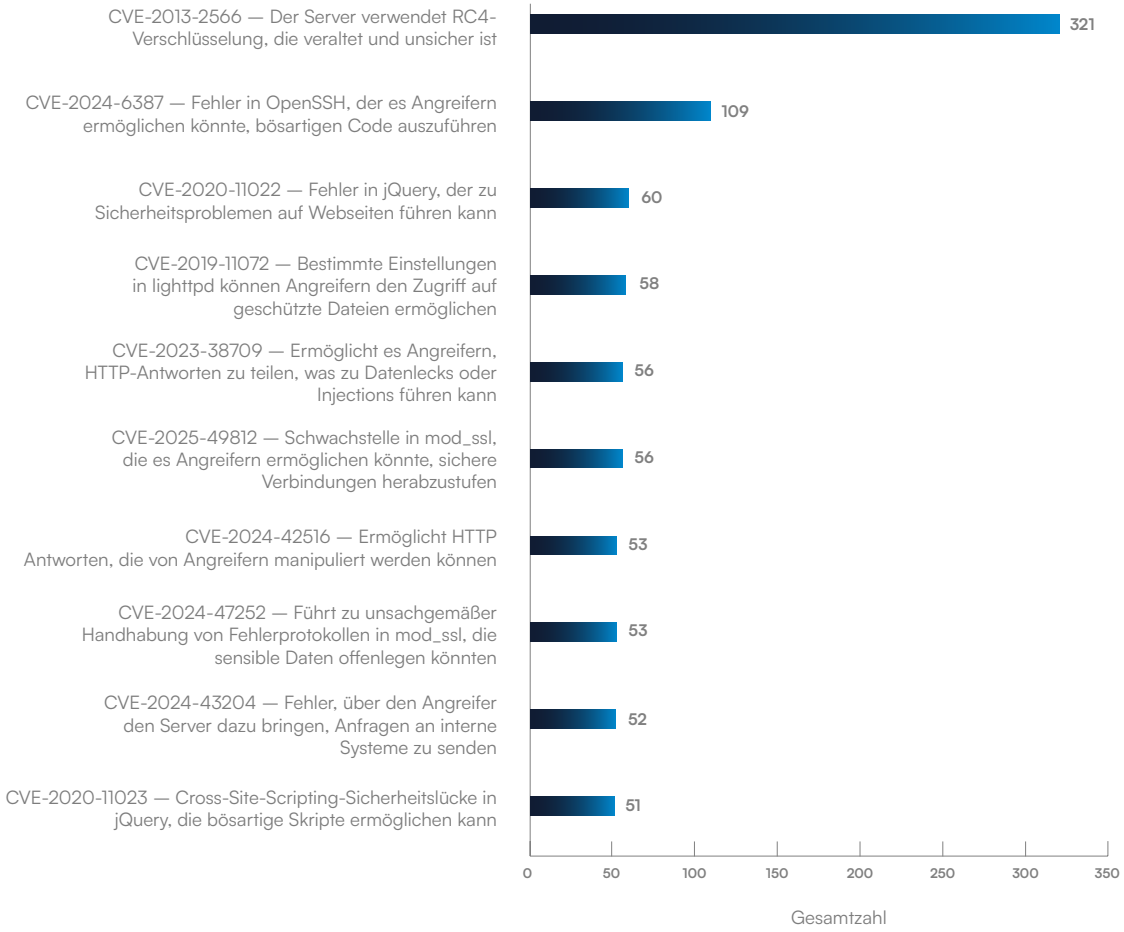


ABBILDUNG 4

Gefundene Top-Schwachstellen mit einer zugewiesenen CVE in Organisationen

Die am häufigsten entdeckte Schwachstelle ist gleichzeitig die älteste. CVE-2013-2566 existiert seit fast 13 Jahren und ist immer noch in älteren Systemen wie alten Servern, eingebetteten Geräten oder Anwendungen zu finden.

Diese Systeme können aktiv genutzt werden, sind aber oft inaktiv und vergessen. Die Prävalenz dieser Schwachstelle ist eine deutliche Warnung vor dem Risiko einer ruhenden Exposition. Je früher eine Schwachstelle gepatcht wird, desto geringer ist die Wahrscheinlichkeit, dass sie übersehen wird.

Nur eine CVE auf der Liste hat eine kritische Schweregradbewertung, aber fünf sind als hoch eingestuft. Der durchschnittliche Schweregrad aller in den letzten 12 Monaten entdeckten Schwachstellen lag bei 5,9.

CVE-2013-2566 — Der Server ist auf eine anfällige und veraltete RC4-Verschlüsselung angewiesen

Schweregrad: **MITTEL**

Angreifer können es nutzen, um:

Schwache Verschlüsselung auszunutzen, um sensible Daten in Klartext zu entschlüsseln. RC4 ist eine Art Verschlüsselungschiffre.

So bleiben Sie sicher:

Deaktivieren Sie RC4 in TLS-Konfigurationen (siehe oben) und verwenden Sie moderne Verschlüsselungen wie AES, TLS 1.2+.

CVE-2024-6387 — Fehler in OpenSSH, der es Angreifern ermöglichen könnte, bösartigen Code auszuführen

Schweregrad: **KRITISCH**

Angreifer können es nutzen, um:

Die vollständige Kontrolle über die betroffenen Systeme aus der Ferne zu erlangen. SSH ist Secure Shell, ein Protokoll zur sicheren Verbindung mit entfernten Systemen über ein ungesichertes Netzwerk wie das Internet, und OpenSSH ist eine freie, quelloffene Version.

So bleiben Sie sicher:

Wenden Sie sofort die neuesten OpenSSH-Patches an und beschränken Sie den SSH-Zugang.

CVE-2020-11022 — Ein Fehler in jQuery, der zu Sicherheitsproblemen auf Webseiten führen kann

Schweregrad: **MITTEL**

Angreifer können es nutzen, um:

Bösartige Skripte in Webseiten zu injizieren und Sitzungen und Daten zu stehlen. jQuery ist eine JavaScript-Bibliothek, die das Programmieren für Entwickler erleichtert.

So bleiben Sie sicher:

Aktualisieren Sie auf die neueste Version von jQuery und bereinigen Sie die Daten, bevor Ihr System sie verwendet.

CVE-2019-11072 — Bestimmte Einstellungen im lighttpd-Webserver können Angreifern den Zugriff auf geschützte Dateien ermöglichen

Schweregrad: **HOCH**

Angreifer können es nutzen, um:

Auf eingeschränkte Dateien auf dem Server, einschließlich sensibler Konfigurationen oder Daten, zuzugreifen. Ein lighttpd-Server ist ein Open-Source-Webserver, der für geschwindigkeitskritische Umgebungen entwickelt wurde.

So bleiben Sie sicher:

Aktualisieren Sie den lighttpd-Webserver auf die neueste Version und stellen Sie sicher, dass alle von den Nutzern angegebenen Dateistandorte überprüft und bereinigt werden, um Missbrauch zu vermeiden.

CVE-2023-38709 — Ermöglicht es Angreifern, HTTP-Antworten in verwundbaren Apache-Webservern zu teilen, was möglicherweise zu Datenlecks oder Injektionen führt

Schweregrad: **HOCH**

Angreifer können es nutzen, um:

Gefälschte Anweisungen zu Webantworten hinzuzufügen, Systeme dazu zu verleiten, schädliche Daten zu speichern, oder bösartigen Code in Webseiten zu injizieren, wodurch die Datenintegrität und die Security der Nutzer gefährdet werden.

So bleiben Sie sicher:

Aktualisieren Sie den Apache-Webserver und stellen Sie sicher, dass alle Browser-zu-Server-Anweisungen oder Header-Daten ordnungsgemäß überprüft und bereinigt werden.

CVE-2025-49812 — Schwachstelle in mod_ssl, die es Angreifern ermöglichen könnte, sichere Verbindungen herabzustufen

Schweregrad: **HOCH**

Angreifer können es nutzen, um:

Den Verschlüsselungsgrad herabzusetzen oder den Datenverkehr abzufangen und sensible Daten preiszugeben. mod_ssl ist ein Apache HTTP-Server-Modul, das Unterstützung für Verschlüsselung hinzufügt.

So bleiben Sie sicher:

Wenden Sie die neuesten Apache-Patches an und setzen Sie starke TLS-Verschlüsselungskonfigurationen durch.

CVE-2024-42516 — Eine Sicherheitslücke, die es Angreifern ermöglicht, HTTP-Webantworten, die an Nutzer gesendet werden, zu manipulieren

Schweregrad: **HOCH**

Angreifer können es nutzen, um:

Schwächen darin auszunutzen, wie ein System Daten empfängt, prüft und verarbeitet, um schädliche Inhalte oder Weiterleitungen einzuschleusen, die zu Phishing, Malware-Lieferung oder gestohlenen Nutzersitzungen führen können.

So bleiben Sie sicher:

Wenden Sie Hersteller-Patches umgehend an und erzwingen Sie starke Sicherheits-Header.

CVE-2024-47252 — Führt zu unsachgemäßer Handhabung von Fehlerprotokollen in mod_ssl, die sensible Daten offenlegen könnten

Schweregrad: **MITTEL**

Angreifer können es nutzen, um:

Bösartige Inhalte in Protokolle einzufügen, die Protokolle vergiften und möglicherweise Rechte erweitern können.

So bleiben Sie sicher:

Aktualisieren Sie Apache und schränken Sie den Protokollzugriff ein.

CVE-2024-43204 — Ein Fehler, über den Angreifer den Server dazu bringen, Anfragen an interne Systeme zu senden

Schweregrad: **HOCH**

Angreifer können es nutzen, um:

Einen Server zu zwingen, Anfragen an interne Systeme zu stellen, wodurch das interne Netzwerk offengelegt wird.

So bleiben Sie sicher:

Patchen Sie Apache und validieren Sie die Header-Konfigurationen.

CVE-2020-11023 — Cross-Site-Scripting-Sicherheitslücke in jQuery, die bösartige Skripte ermöglichen kann

Schweregrad: **MITTEL**

Angreifer können es nutzen, um:

Bösartige Skripte einzuschleusen.

So bleiben Sie sicher:

Aktualisieren Sie jQuery, bereinigen Sie Nutzereingaben und verwenden Sie Tools, um schädlichen Code zu blockieren.

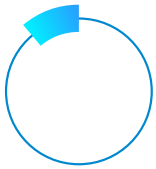
Zusätzliche Erkenntnisse von Barracuda Managed Vulnerability Security

4.146

Gesamtzahl der erkannten kritischen Schwachstellen.

2.525

Gesamtzahl der identifizierten einzigartigen Schwachstellen.



11 %

Anteil der Schwachstellen, für die ein Exploit bekannt ist.

Vorfallbericht — Ungepatchte Firewall bei RansomHub-Angriff verwendet

Die Angreifer nutzten ungepatchte Schwachstellen in einer Fortinet-Firewall aus. Sie starteten Brute-Force-Aktivitäten gegen das Netzwerk eines Kunden, wurden aber blockiert. Einen Monat später versuchten sie eine Fernanmeldung (SSL-VPN), wurden aber erneut blockiert. Zwei Tage später unternahmen sie einen dritten Versuch. Barracuda Managed XDR erkannte PsExec-Aktivitäten (Remote-Befehle) und fand bösartige Software auf dem primären Domänencontroller und dem Backup-Server.

Fehlkonfiguration: Vorfälle, bei denen Security-Tools versehentlich oder absichtlich deaktiviert wurden

Sicherheitstools, die nicht richtig konfiguriert wurden, stellen ein großes Sicherheitsrisiko dar. Die Gefahr kann durch das falsche Gefühl der Sicherheit, das durch die Installation des Werkzeugs entsteht, noch verstärkt werden. In den letzten 12 Monaten identifizierte Barracuda Managed XDR deaktivierte Funktionen, darunter Endpunktschutzagenten (die 94 % der deaktivierten Security-Erkennungen ausmachten), MFA (3,62 %), Safe Link (1,4 %) und sichere Anbindungsregeln (0,6 %).

Studien zeigen, dass die meisten Unternehmen versuchen, zu viele Security-Tools zu verwalten. Wenn Ressourcen knapp sind, können Konfigurationsfehler leicht auftreten. Der beste Schutz ist eine integrierte Sicherheitsplattform mit vollem Überblick über Einstellungen und Konfigurationen, die schnell und automatisch Lücken erkennen kann, die behoben werden müssen.

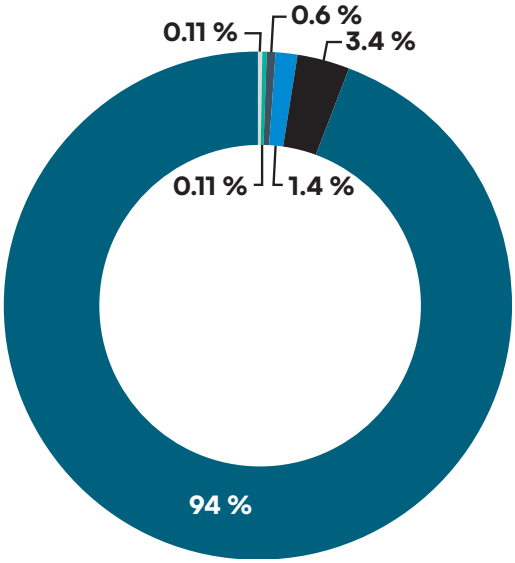


ABBILDUNG 5

Die am häufigsten deaktivierten Sicherheitsfunktionen

- SentinelOne Endpoint Agent deaktiviert
- Microsoft 365 MFA deaktiviert
- Microsoft 365 ATP-Regel für „sichere Links“ deaktiviert
- Microsoft Office ATP „Safe Attachment“-Regel deaktiviert
- Microsoft Azure MFA deaktiviert
- Google Workspace MFA deaktiviert

100 %

Anteil der Vorfälle, auf die Barracuda Managed XDR reagiert hat und die mindestens einen ungeschützten oder nicht autorisierten Endpunkt betrafen

66 %

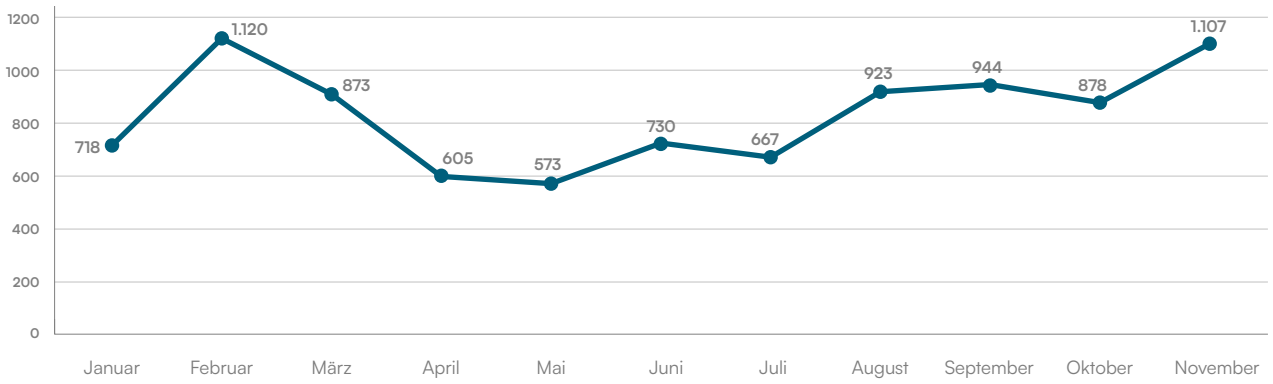
Anteil der Vorfälle, auf die Barracuda Managed XDR reagierte und die die Lieferkette oder eine dritte Partei betrafen (Anstieg gegenüber 45 % im Jahr 2024)

Die anhaltende Bedrohung durch Ransomware

In den letzten 12 Monaten hat Barracuda Managed XDR 13.514 Indikatoren identifiziert, die auf einen laufenden Ransomware-Angriff hindeuten, darunter Tools, Techniken und Verhaltensweisen. Im Gegensatz zu den Vorjahren gibt es keine ausgeprägten Spitzen oder Tiefpunkte mehr, sondern ein konstant hohes Niveau an Vorfällen das ganze Jahr über.

ABBILDUNG 6

Vorfälle im Zusammenhang mit Ransomware 2025



1.5 % bis 5.6 %

Anteil aller Organisationen, die jeden Monat im Jahr 2024 von Ransomware betroffen sind

5.1 % bis 10.9 %

Anteil aller Organisationen, die jeden Monat im Jahr 2025 von Ransomware betroffen sind

Die häufigsten Ransomware-Familien im Jahr 2025

Akira

- Akira ist eine relativ neue Ransomware-Gruppe, die dafür bekannt ist, Organisationen mit ausgeklügelten Angriffen anzugreifen. Sie setzt oft Doppelerpressungstaktiken ein, verschlüsselt Daten und droht mit der Veröffentlichung sensibler Informationen, wenn kein Lösegeld gezahlt wird.
- **Taktiken**: Einsatz hochentwickelter Malware, gezielte Angriffe und Datendiebstahl.

Qilin

- Qilin ist eine Ransomware-Gruppe, die durch gezielte Angriffe auf kritische Infrastrukturen und Unternehmensorganisationen Aufmerksamkeit erregt hat.
- **Taktiken**: Doppelte Erpressung, Ausnutzung von Schwachstellen und Einsatz von Malware zur Datenverschlüsselung.

RansomHub

- RansomHub ist eine Ransomware-Operation, die als Ransomware-as-a-Service (RaaS) operiert und es Partnern ermöglicht, Ransomware unter ihrer eigenen Marke einzusetzen.
- **Taktiken**: Ransomware-as-a-Service-(RaaS-)Modell, Datendiebstahl und Erpressung.

Cactus

- Cactus ist eine Ransomware-Gruppe, die an gezielten Angriffen beteiligt war und oft hohe Lösegelder fordert.
- **Taktiken**: Datenverschlüsselung, doppelte Erpressung und Ausnutzung von Schwachstellen.

Vorfallbericht — Mehrere Security-Lücken setzen das Ziel Cactus aus

Die Ziele wurden durch Teams-Anrufe dazu verleitet, bösartige Dateien herunterzuladen. Die Angreifer richten Kanäle ein, um aus der Ferne Befehle zu erteilen, sich seitlich zu bewegen und Persistenz zu erhalten. Bösartige geplante Aufgaben, Registry-Bearbeitungen und DLL-Sideloading (wenn ein Programm dazu gebracht wird, eine gefälschte, schädliche gemeinsame Codedatei zu laden, sodass der Code des Angreifers statt des echten läuft) halfen den Angreifern, Privilegien zu erhöhen und der Erkennung zu entgehen. Das Barracuda Managed XDR-Team entdeckte unbefugte Geräte und mehr als 1.600 ungeschützte Geräte im Netzwerk, lasche Microsoft Teams-Berechtigungen, anfällige Bereitstellungen des Remote Desktop Protocol (RDP) und Secure Shell, unsignierte Dateien sowie ein mangelndes Bewusstsein der Mitarbeiter.

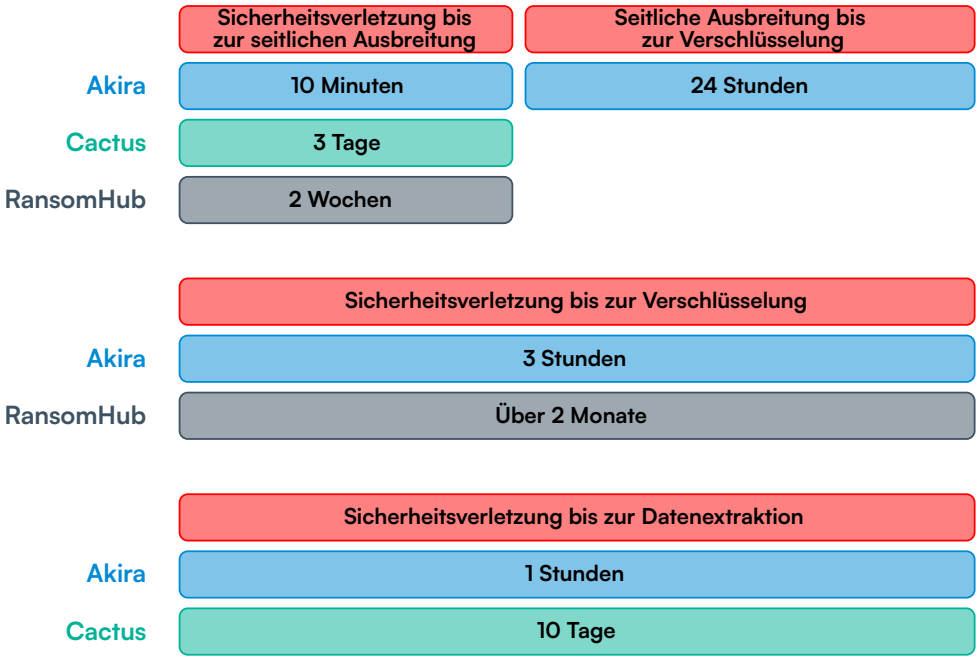
Ransomware bewegt sich mit unterschiedlichen Geschwindigkeiten

Laut den Erkennungs- und Vorfalldaten von Barracuda Managed XDR dauerten die schnellsten Ransomware-Angriffe im Jahr 2025 durchgehend nur Stunden, während die längsten Monate dauerten.

Langwierige Eingriffe ermöglichen maximalen Schaden, da Angreifer Zeit für Aufklärung, Datenexfiltration, Sabotage und mehr haben. Vorfälle, die sich blitzschnell entwickeln, sind schwieriger zu erfassen und einzudämmen, bevor sie ausgeführt wurden und der Schaden entstanden ist.

Organisationen müssen auf beide Arten von Angriffen vorbereitet sein — und über Sicherheits-Tools verfügen, die stets auf der Hut sind.

Die Geschwindigkeit von Ransomware — 3 Akteure



Geschätzte Zeiten anhand von Vorfällen in der realen Welt

Vorfallbericht — XDR entdeckt Akira-Ransomware, die ein „Geisterkonto“ und einen ungeschützten Server ausnutzt

Die Angreifer drangen über ein Konto in das Netzwerk ein, das für einen Drittanbieter erstellt wurde und nicht deaktiviert wurde, als dieser das Unternehmen verließ. Die Angreifer versuchten, sich seitlich zu bewegen und die Endgeräte-Security zu deaktivieren, wurden aber blockiert. Sie wechselten auf einen ungeschützten Server, erweiterten ihre Berechtigungen und starteten die Ransomware. Alle betroffenen Geräte wurden neutralisiert. Weitere Risiken im Zielnetzwerk waren ungeschützte Geräte, ein offener VPN-Kanal in der Firewall und inkonsistente MFA.

Fazit: So bleiben Sie in einer Welt komplexer Bedrohungen sicher

Security-Teams stehen vor wachsenden Herausforderungen. Mit begrenzten Ressourcen müssen sie eine sich ständig erweiternde Landschaft von Geräten, Anwendungen, kritischen Schwachstellen und fragmentierten Security-Tools schützen, oft ohne den einheitlichen Überblick, den sie brauchen, um Bedrohungen einen Schritt voraus zu sein.

Alles wird noch schwieriger, da Angreifer beginnen, agentische KI zu nutzen.

Agentische KI-Systeme werden die frühen und sich wiederholenden Phasen eines Angriffs automatisieren, Umgebungen nonstop scannen, schwache Konfigurationen identifizieren und gezielte Exploits in Minutenschnelle starten. Bedrohungsakteure, die KI-Agenten nutzen, können Entscheidungen treffen, Strategien anpassen und bösartigen Code korrigieren oder neu schreiben, wenn etwas fehlschlägt oder sie auf ein Hindernis stoßen. Diese Änderung wird die Geschwindigkeit, den Umfang und die Konstanz der Angriffe drastisch erhöhen.

Unternehmen benötigen eine einheitliche Security-Strategie, die fortschrittliche, KI-gestützte Erkennungstechnologien mit einem vollständig autonomen SOC integriert und durch Nutzer-Schulung, automatisierte Reaktion auf Bedrohungen und eine widerstandsfähige Security-Kultur ergänzt wird.

Es gibt schnelle Erfolge, wie jene, die in diesem Bericht beschrieben werden. Sie umfassen eine konsistente Multifaktor-Authentifizierung und Zugriffskontrollen, einen robusten Ansatz für Patch-Management und Datenschutz sowie regelmäßige Schulungen zur Cybersicherheitsaufklärung für Mitarbeitende.

Dies sollte durch eine umfassende, verwaltete Security-Plattform und eine 24/7 verwaltete XDR-Lösung untermauert werden, die Netzwerk-, Endpunkt-, Server-, Cloud- und E-Mail-Sicherheit integriert — und so vollständige End-to-End-Transparenz und Managementkontrolle bietet, unterstützt durch ein vollständig autonomes SOC.

Langfristige Security liegt in der Cyber-Resilienz. Erkennung und Prävention sind die Grundpfeiler jeder Sicherheitsstrategie, doch angesichts zunehmend komplexer und ausweichender Bedrohungen ist es entscheidend, schnell und mit minimalen Auswirkungen auf Angriffe zu reagieren und sich von ihnen zu erholen.

Die Ergebnisse in diesem Bericht basieren auf Erkennungsdaten von Barracuda Managed XDR, einer erweiterten Plattform für Sichtbarkeit, Erkennung und Reaktion (XDR), die von einem Security Operations Center (SOC) unterstützt wird, das Kunden rund um die Uhr menschliche und KI-gestützte Dienste zur Bedrohungserkennung, Analyse, Incident Response und Schadensbegrenzung bietet.

Barracuda Managed XDR ist Teil von BarracudaONE, einer KI-gestützten Plattform, die E-Mails, Daten, Anwendungen und Netzwerke mit innovativen Lösungen und einem zentralen Dashboard schützt, um den Schutz zu maximieren und die Cyber-Resilienz zu stärken.

Über Barracuda

Barracuda ist ein weltweit führendes Cybersecurity-Unternehmen, das umfassenden Schutz vor komplexen Bedrohungen für Unternehmen aller Größen bietet. Unsere KI-gestützte Plattform BarracudaONE schützt E-Mails, Daten, Anwendungen und Netzwerke mit innovativen Lösungen, einem Managed XDR-Service sowie einem zentralen Dashboard. Das sorgt für maximalen Schutz und stärkt die Cyber-Resilienz. Von Hunderttausenden von IT-Experten und Managed Service Providern weltweit als vertrauenswürdig angesehen, bietet Barracuda leistungsstarke Abwehrmaßnahmen, die einfach zu kaufen, bereitzustellen und zu verwenden sind.