



synalis Die Kunst der IT

Ransomware bedroht Ihr Business

10 Wege, wie sich Unternehmen mit Zero Trust davor schützen

✘ **Bei 50 % aller Ransomware-Angriffe kommt es zu einer Doppelerpressung.**

Jeder Ransomware-Angriff ist jetzt auch eine mögliche Datenpanne.

✘ **Alle 14 Sekunden wird irgendwo auf der Welt ein Angriff ausgeführt.**

Alle Unternehmen sind gefährdet, wobei sich Umfang und Anzahl der Angriffe sprunghaft erhöhen.

✘ **Seit Anfang 2020 ist die Anzahl verschlüsselter Ransomware um mehr als 500 % gestiegen.**

Dabei werden Angriffe verschleiert, um herkömmliche Sicherheitskontrollen zu umgehen.

Ransomware-Angriffe sind die größte Bedrohung für die digitale Wirtschaft

Ransomware-Angriffe finden zwar schon seit Jahrzehnten statt, doch in den letzten Jahren haben sie sprunghaft zugenommen. Wurden Ransomware-Angriffe früher von Einzeltätern durchgeführt, erfolgen sie heute systematisch durch vernetzte Gruppen, die untereinander gegen Bezahlung ihr Wissen und ihre Werkzeuge austauschen. Waren solche Attacken in der Vergangenheit unspezifisch und eindimensional, werden heute gezielte und vielschichtige Strategien eingesetzt. Diese Entwicklung erschwert die Abwehr erheblich. Auch die Höhe der geforderten Lösegelder sind immens gestiegen. **Schätzungen zufolge wird Ransomware bis Ende 2024 Schäden in Höhe von 42 Milliarden USD verursachen.**¹

Der wohl folgenreichste neue Trend bei modernen Ransomware-Angriffen ist die Double Extortion (doppelte Erpressung), bei der Daten nicht nur verschlüsselt, sondern auch entwendet werden, damit die Angreifer zusätzlich mit der Veröffentlichung dieser Daten drohen können. Bei etwa der Hälfte aller Ransomware-Angriffe wird heute auch versucht, Daten auszuschleusen.

Allerdings gibt es eine Strategie, mit der Unternehmen die Chancen erhöhen können, die schädlichen Auswirkungen von Ransomware-Angriffen abzumildern: Zero Trust.

Dieser Sicherheitsansatz geht von der Annahme aus, dass die Angreifer bereits in das System eingedrungen sind. Dementsprechend werden Architekturen, Richtlinien für die Zugangskontrolle sowie Überwachungs- und Authentifizierungsmaßnahmen eingeführt, die dafür sorgen sollen, dass sich Umfang und Schwere des von einem Angreifer verursachten Schadens möglichst in Grenzen halten.

Im Folgenden werden zehn verschiedene Möglichkeiten vorgestellt, wie sich Unternehmen mit Zero Trust vor Ransomware-Angriffen schützen können. ✘

¹ Laut Cybersecurity Ventures wird „Ransomware bis 2031 weltweit voraussichtlich Schäden in Höhe von mehr als 265 Milliarden USD verursachen“.

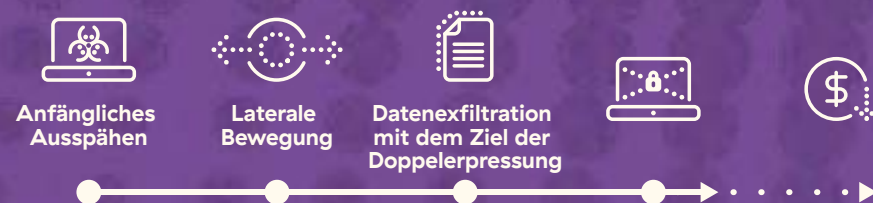
Ablauf von Ransomware-Angriffen – und wie man sie vereitelt.

Soll ein Ransomware-Angriff erfolgreich sein, muss eine Reihe von Bedingungen erfüllt sein. Zunächst müssen Angreifer ein System mit einer schädlichen Ransomware-Payload infizieren, um sich Zugang zur IT-Umgebung zu verschaffen. **Das erste Mittel zur Vereitelung eines solchen Angriffs sind daher vorbeugende Kontrollen, die Sicherheitsrisiken beseitigen, die Angriffsfläche reduzieren und es ermöglichen, Traffic zu blockieren, zu steuern und zu überprüfen.**

Bevor Angreifer zuschlagen, sondieren sie die Lage, um die Daten auszumachen, deren Entwendung und Verschlüsselung für sie besonders lohnend ist. Dafür müssen sie sich lateral durch das Netzwerk bewegen können. **Der zweite Schritt zur Abwehr eines Angriffs und zur Abmilderung der Folgen besteht deshalb darin, Angreifer in ihrer lateralen Bewegungsfähigkeit einzuschränken.**

Bei einem Angriff mit doppelter Erpressung werden Daten gestohlen und „als Geisel“ genommen, um die Erfolgchancen der Attacke zu verbessern und die Lösegeldforderung in die Höhe treiben zu können. **Die dritte Schutzmaßnahme ist daher die Methode der Data Loss Prevention.**

Als Nächstes schauen wir uns an, wie Zero Trust Ihr System entlang der Abfolge von Angriffsphasen schützt.



Nr. 1

Eine Zero Trust Architektur macht Anwendungen für die Angreifer unsichtbar. Und was man nicht sehen kann, kann man auch nicht angreifen.

Wenn Anwendungs-, User- und Geräteidentitäten im Internet ungeschützt auffindbar sind, werden die wertvollsten Informationen offen zur Schau gestellt. Leichter kann man Angriffe nicht provozieren. Sind diese Daten sichtbar, können Angreifer sie leicht aufspüren und Sicherheitsrisiken — wie ungepatchte Webserver-Software oder schwache Passwörter, die per Brute-Force-Angriff geknackt werden können — ausnutzen. Hacker und Cyberkriminelle können sich so sofort problemlos Zugang zu einer IT-Umgebung verschaffen.

Bei einer Lösung wie Zscaler Private Access™ stellt die Anwendung die Verbindung zum User her, nicht umgekehrt. Da die Verbindung von innen nach außen hergestellt wird, sind Anwendungen nicht öffentlich und somit für Angreifer unsichtbar. Wird diese Herangehensweise auf alle Geräte und Anwendungen in einer Umgebung angewandt, ist es für Angreifer praktisch unmöglich, diese im Vorfeld auszuspähen.

Nr. 2

Bei einer Zero Trust Architektur wird der gesamte Traffic — einschließlich des verschlüsselten Datenverkehrs — umfassend und gründlich überprüft.

Mehr als 90 % des Internet-Traffics sind inzwischen verschlüsselt. Schädlicher Datenverkehr bildet hier keine Ausnahme, und die Menge verschlüsselter Ransomware ist seit Anfang 2020 um mehr als 500 % gestiegen. Sicherheitsteams, die bisher einfach darauf vertraut haben, dass SSL-verschlüsselter Traffic harmlos ist, müssen umdenken.

Wesentlicher Bestandteil einer soliden Verteidigungsstrategie ist daher die Überprüfung des gesamten Traffics, inklusive der verschlüsselten Daten. Doch Architekturen, die auf Firewalls der nächsten Generation und andere perimeterbasierte Verteidigungsmaßnahmen setzen, sind dieser Aufgabe nicht mehr gewachsen. Selbst die fortschrittlichsten On-Premise-Sicherheitstools sind nicht in der Lage, den gesamten SSL-verschlüsselten Traffic zu überprüfen, ohne Performance-Engpässe zu verursachen. Und diese bremsen die Produktivität aus.

Abhilfe schafft hier eine Proxy-basierte Architektur in der Cloud, die speziell für die Erkennung SSL-verschlüsselter Malware in großem Maßstab entwickelt wurde. Sie schützt den gesamten Traffic und beseitigt überdies Schwachstellen.

Die beste Strategie ist, Bedrohungen zu erkennen, bevor sie Schaden anrichten können: Zero Trust schützt vor Ransomware, die so neu ist, dass sie noch keiner kennt.

Eine wachsende Zahl von Ransomware-Angriffen macht sich speziell entwickelte Malware zunutze. Um sich vor dieser Bedrohung zu schützen, muss man in der Lage sein, neue Bedrohungen zu erkennen und zu blockieren. Mit Cloud-nativem Sandboxing und KI-gestützter Erkennung können Verhaltensanalysen durchgeführt werden, um bisher unbekannte Ransomware-Varianten zu entdecken. Dabei werden Dateien erst vollständig isoliert und analysiert, bevor sie an Nutzer übermittelt oder ausgeführt werden dürfen.

Mit einer Lösung wie der Zscaler Cloud Sandbox können Richtlinien nach Usern, Gruppen und Inhaltskategorien definiert werden, was eine granulare Steuerung der Quarantänemaßnahmen ermöglicht. Da diese Lösung Teil der Zscaler Zero Trust Exchange™ ist, erhalten Unternehmen nahezu in Echtzeit Dateibewertungen einer globalen Community. Damit werden die Auswirkungen auf User minimiert und gleichzeitig die größtmögliche Treffsicherheit bei der Malware-Erkennung gewährleistet.

Vereinfachte Zugriffskontrollrichtlinien durch Mikrosegmentierung: Zero Trust erhöht Transparenz und Wirksamkeit.

Ein Kernkonzept des Zero Trust Modells ist die Mikrosegmentierung. Dabei wird der Zugriff auf Anwendungen und Ressourcen beschränkt, damit eindringende Angreifer keinen Schaden bei anderen Anwendungen und Ressourcen anrichten können. Beim herkömmlichen netzwerk-basierten Ansatz der Mikrosegmentierung wurden Regeln von Firewalls mittels Prüfung von Netzwerkadressen durchgesetzt. Doch dieser Ansatz erforderte jedes Mal eine Neudefinition und Aktualisierung der Richtlinien, wenn Anwendungen verschoben und Netzwerke weiterentwickelt wurden. Das stellte schon in On-Premise-Rechenzentren eine Herausforderung dar, aber die für die Cloud typische Kurzlebigkeit hat die Komplexität so stark erhöht, dass sie nicht mehr zu bewältigen ist.

Proxy-Architekturen reduzieren die Komplexität bei der Implementierung von Mikrosegmentierung erheblich und bieten zugleich einen stabileren Schutz für Workloads. Richtlinien und Berechtigungen werden auf Grundlage von Ressourcenidentitäten verwaltet, sodass sie von der zugrunde liegenden Netzwerkinfrastruktur unabhängig sind und sich automatisch anpassen können — ganz gleich, wie dynamisch die Netzwerkarchitektur ist oder wie schnell sich Geschäftsanforderungen ändern. Außerdem wird dadurch die Verwaltung vereinfacht, da zum Schutz eines Segments statt hunderter adressbasierter Regeln nur noch wenige identitätsbasierte Richtlinien erforderlich sind.



Eine Zero Trust Architektur schützt Nutzer und Geräte standortunabhängig.

Als für Unternehmen aller Branchen aufgrund der COVID-19-Pandemie Remote-Arbeit unumgänglich wurde, setzten viele Unternehmen auf Virtual Private Networks (VPNs) oder das Remote Desktop Protokoll (RDP), um Mitarbeitenden im Homeoffice den Zugriff auf Unternehmensnetzwerke und -ressourcen zu ermöglichen. Hacker passten ihre Ransomware-Angriffe deshalb innerhalb kürzester Zeit an und starteten eine neue Welle von RDP- und VPN-basierten Angriffen. Tatsächlich wurden bei dem berüchtigten Angriff auf die Colonial Pipeline die Schwachstellen eines VPN ausgenutzt. Und das brachte fast die Hälfte der Kraftstoffversorgung im Osten der USA zum Erliegen.

Bei einem Zero Trust Ansatz zum Schutz von Mitarbeitenden, die remote auf Daten und Anwendungen zugreifen, wird jede Verbindung gleichermaßen geschützt. Es spielt keine Rolle, wo sich die Mitarbeitenden befinden. Dabei werden alle Geräte eines Mitarbeitenden um den ressourcenschonenden Endgeräte-Agent Zscaler Client Connector ergänzt. Mit diesem Instrument erhalten sie Zugang zu allen über die Zscaler Zero Trust Exchange verfügbaren Sicherheitsmaßnahmen, Möglichkeiten zur Richtliniendurchsetzung und Zugriffskontrollen. Da Zscaler weltweit über 150 Rechenzentren verteilt ist, profitieren alle immer von einer schnellen Verbindung über ein nahegelegenes Rechenzentrum, ohne die durch VPNs verursachte Latenz.

Echte Zero Trust Architekturen verhindern, dass sich Angreifer lateral durch Ihr Netzwerk bewegen.

Um schädlichen Traffic von Unternehmensnetzwerken fernzuhalten, verlassen sich zu viele Sicherheitsteams immer noch auf herkömmliche Firewall-basierte Netzwerksegmentierung. Doch die Implementierung und Verwaltung solcher Strategien ist aufwendig und bietet keinen ausreichenden Schutz für interne Ressourcen. Gelingt es Angreifern, bis zu einer Anwendung vorzudringen oder eine Firewall zu durchbrechen, können sie sich immer noch in der IT-Umgebung ungehindert ausbreiten und haben so vermehrt die Möglichkeit, mehr Daten zu verschlüsseln und zu entwenden.

Bei einem echten Zero Trust Modell werden Mitarbeitende direkt mit einer Anwendung verbunden, ohne dabei ins Netzwerk zu gelangen. Für diese direkte Verbindung und die kontinuierliche Authentifizierung der Mitarbeitenden können Sicherheitsteams eine Proxy-Architektur einsetzen, anstatt Traffic aus einem internen Netzwerk oder Subnetz zu vertrauen. Dadurch wird die größte digitale Bedrohung beseitigt, der Unternehmen heute ausgesetzt sind. Das Beste daran: Ein Proxy funktioniert unabhängig davon, wo sich Mitarbeitende, Geräte oder Anwendungen befinden, und bietet sowohl On-Premise als auch remote immer eine sichere Verbindung.

Eine Zero Trust Architektur verhindert durch Einhaltung der Unternehmensrichtlinien, dass sich Angreifer Workloads zunutze machen.

In einer Zero Trust Architektur werden Sicherheitsrichtlinien gemäß der Identität der Workloads durchgesetzt, die versuchen, miteinander zu kommunizieren. Diese Identitäten werden ständig überprüft. Nicht verifizierte Workloads werden gesperrt, sodass sie nicht mit anderen Workloads kommunizieren können. So können diese weder mit schädlichen Remote-Command-and-Control-Servern noch mit internen Hosts, Mitarbeitenden, Anwendungen und Daten interagieren.

Eine Plattform wie die Zscaler Zero Trust Exchange stellt automatisch sicher, dass der gesamte Traffic, unabhängig von der Herkunft, beim Zugriff auf Ressourcen alle Unternehmensrichtlinien einhält. Die Plattform wendet diese Richtlinien durchgängig einheitlich an, ganz gleich, ob es sich um interne oder externe Ressourcen oder externe SaaS-Lösungen handelt. Das ist im Vergleich zur mehrschichtigen Durchsetzung von Richtlinien nicht nur eine viel einfachere, sondern auch eine weitaus effektivere Methode zur Netzwerkmikrosegmentierung.

Das Zero Trust Modell umfasst proaktive Strategien, um den Gegner mit seinen eigenen Waffen zu schlagen.

Hacker, die heutzutage Ransomware-Angriffe verüben, sind raffiniert und können grundlegende Schutzmaßnahmen problemlos umgehen. Zur grundlegenden Strategie des Zero Trust Modells gehört deshalb das Aufspüren und Eingrenzen von Angriffen, bevor diese Schaden anrichten. Als weltweit einzige Zero Trust Plattform mit integrierter Deception Technology nutzt Zscaler Deception™ fortschrittliche Taktiken, um Angreifer zu ködern, zu erkennen und abzufangen — wie raffiniert oder zielgerichtet ihre Strategien auch sein mögen.

Bei diesem proaktiven Verteidigungsansatz wird Ihre IT-Umgebung mit Attrappen wie gefälschten Endgeräten, Verzeichnissen, Datenbanken, Dateien und Benutzerpfaden versehen. Diese Attrappen imitieren hochwertige Produktionsvorrichtungen, bleiben den echten Mitarbeitenden aber verborgen. Ihr alleiniger Zweck besteht darin, Ihr Sicherheitsteam bei Kontakt mit Angreifern zu warnen. Da diese Attrappen nicht in den legitimen Datenverkehr eingebunden sind, funktionieren die Warnungen extrem zuverlässig. Sie liefern den konkreten Nachweis für eine Bedrohung oder ein Datenleck und ragen so aus der Masse der Meldungen anderer Erkennungssysteme heraus. Dies verschafft Ihrem Sicherheitsteam einen Vorteil und erlaubt es ihm, die Pläne der Angreifer zu durchkreuzen und den Schaden auf ein Minimum einzugrenzen.



Zero Trust Architekturen bieten umfassenden Schutz vor Doppelerpressung durch Datenverluste.

Aufgrund der Zunahme von Ransomware-Angriffsstrategien, die auf eine doppelte Erpressung abzielen, muss heute jeder Ransomware-Angriff als Datenschutzverletzung angesehen werden. Maßnahmen zur Verhinderung des Datendiebstahls und der Veröffentlichung dieser vertraulicher Daten können die verheerendsten Folgen von Ransomware-Angriffen deutlich abmildern.

Mit einer CASB-Lösung (Cloud Access Security Broker) können granulare Kontrollen für Cloud-Anwendungen durchgesetzt werden, die Daten im Ruhezustand auf SaaS-Plattformen schützen und sowohl die versehentliche Preisgabe als auch einen Datendiebstahl verhindern. Ein weiterer Vorteil besteht darin, dass gleichzeitig die Transparenz über Cloud-Anwendungen verbessert wird. Damit wird gleichsam die Identifizierung von Sicherheitsrisiken, Fehlkonfigurationen und Schatten-IT, also die Verwendung nicht genehmigter Cloud-Anwendungen, vereinfacht. Mithilfe von DLP-Funktionen (Data Loss Prevention) kann die Datenexfiltration automatisch blockiert und so die Wahrscheinlichkeit einer doppelten Erpressung verringert werden.

Durch eine Zero Trust Architektur mit einer vollständigen Inline-Prüfung des gesamten ausgehenden Traffics stoppen Sie den Datendiebstahl.

Genauso wie Cyberkriminelle Malware in SSL-verschlüsseltem eingehenden Traffic verbergen, können sie Verschlüsselung auch dazu nutzen, um einen Diebstahl sensibler und wertvoller Unternehmensdaten zu verschleiern. Zur Vermeidung von Datenverlusten und zur Identifizierung von Zero Day Schwachstellen, die ein Ausschleusen von Daten erlauben, ist die Möglichkeit, SSL-verschlüsselten Traffic vollständig prüfen zu können, maßgeblich.

Eine auf Zero Trust Architektur aufbauende Lösung wie die Zscaler Zero Trust Exchange stellt sicher, dass jede ein- und ausgehende Verbindung in Ihrer Umgebung einzeln überprüft und abgesichert wird. Eine Cloud-native Proxy-Architektur ermöglicht außerdem eine sehr umfangreiche SSL-Überprüfung, ohne die Performance zu beeinträchtigen oder überzogene Kosten zu verursachen. Dadurch werden die bisherigen Sicherheitslücken beseitigt, die bislang für verheerende Ransomware-Angriffe mit doppelter Erpressung ausgenutzt wurden.

Zero Trust bietet Unternehmen vollumfänglichen Schutz vor Ransomware-Angriffen.

Die Zero Trust Exchange bietet umfassende Verteidigungsmaßnahmen gegen alle Schritte, die für einen erfolgreichen Ransomware-Angriff ausgeführt werden müssen. [Weitere Informationen dazu, wie Zscaler den Zero Trust Ansatz nutzt](#), um Unternehmen umfangreich zu schützen, finden Sie hier:



DIE ABWEHR VON RANSOMWARE-ANGRIFFEN BEGINNT MIT ZERO TRUST

Mit den branchenweit umfassendsten Sicherheitsfunktionen
Unternehmen zuverlässig vor Ransomware-Angriffen schützen.

Mehr erfahren



Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen unter [zscaler.de](https://www.zscaler.de) oder auf Twitter unter [@zscaler](https://twitter.com/zscaler).

synalis

Die Kunst der IT

synalis GmbH & Co. KG

vertrieb@synalis.de

+49 228 9268 0

<https://www.synalis.de/>