Zero Trust – ein Gebot der Stunde

Know-how Die aktuelle Cyberbedrohungslage verlangt nach einem Sicherheitsansatz, der auf implizites Vertrauen verzichtet. Zero Trust setzt jedoch nicht nur technische Lösungen voraus, sondern auch organisatorische Massnahmen und vor allem eine fundierte Strategie.

Von Peter Bernold, Ruedi Kubli und Jürg Hefel

Die Arbeitswelt und die damit verbundene IT unterliegen nicht erst seit Corona einer regelrechten Umwälzung: Arbeitsformen wie Home Office und Hybrid Work, immer mehr Anwendungen und Datenquellen sowie der Einsatz von Cloud-Diensten und privaten Mobilgeräten fordern die IT-Sicherheit in einem bisher unerreichten Mass heraus, denn mit all diesen Errungenschaften erlangen Cyberkriminelle eine massiv erweiterte Angriffsfläche innerhalb und ausserhalb des traditionellen Netzwerkperimeters.

Neue Cybersicherheitsstrategie erforderlich

In einem von zunehmenden und immer raffinierteren Cyberattacken geprägten Umfeld funktioniert der herkömmliche Ansatz, einem Teammitglied nach einer simplen Anmeldung per User-ID und Passwort prinzipiell zu vertrauen und ohne weitere Prüfung Zugriff auf alle relevanten Ressourcen im Firmennetz zu gewähren, nicht mehr – egal, ob es im internen Netz oder aus der Ferne via VPN-Verbindung angemeldet ist. Die Tage des impliziten Vertrauens sind gezählt.

Unter dem Begriff Zero Trust hat sich in den letzten Jahren ein neuer Ansatz etabliert, der das implizite Vertrauen vollständig eliminiert. In einer Zero-Trust-Umgebung wird jeder Zugriff auf Unternehmensressourcen und überhaupt jede digitale Interaktion in allen Phasen kontinuierlich verifiziert und nötigenfalls unterbunden. Dies gilt nicht nur für die Zugriffskontrolle der Benutzer, sondern für alles – von Anwendungen, Cloud-Diensten, Microservices und der gesamten Infrastruktur über die Geräte der Benutzer, Cloud- und IoT-Ressourcen bis hin zu den in der Lieferkette genutzten Ressourcen.

Der Zero-Trust-Ansatz unterstützt die Umsetzung eines Sicherheitskonzepts gemäss dem Cybersecurity-Framework der US-Behörde NIST (National Institute of Standards and Technology) massgeblich und wird von NIST ausdrücklich erwähnt. Quelle: Boll Engineering

Man kann es so sehen, dass eigentlich jedes Unternehmen nicht umhinkommt, mit Zero Trust zu arbeiten. Denn erfolgreiche Ransomware-Angriffe, immer wieder gemeldete Daten-Leaks oder per Phishing erlangte und im Darknet verkaufte persönliche Informationen zeigen überdeutlich, dass herkömmliche Sicherheitsmassnahmen nur noch begrenzten Nutzen bringen.

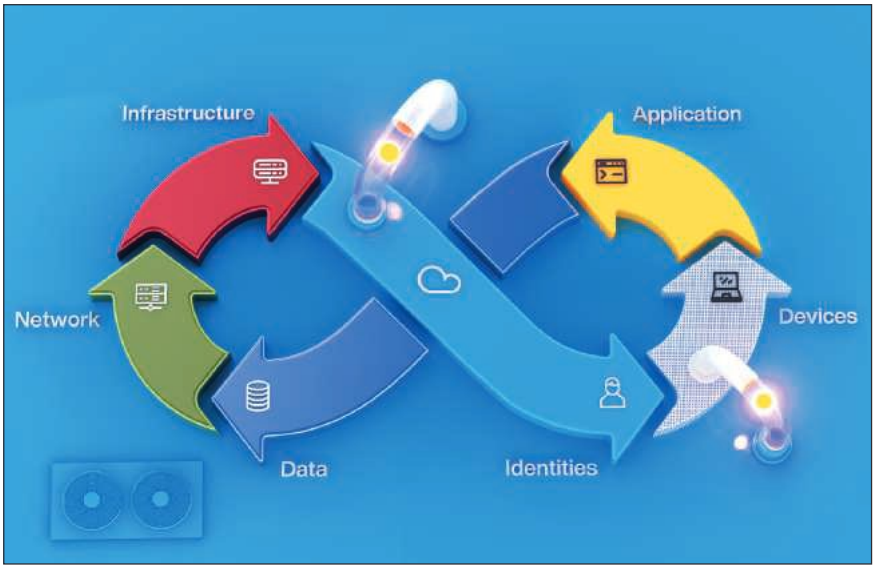
Zero Trust ist mehr als Technik

Eine wirksame Zero-Trust-Strategie ist somit nicht mit der blossen Installation einer starken Authentifizierungslösung umgesetzt. Sie erfordert Massnahmen in verschiedenen Bereichen der IT, aber auch über die IT hinaus. Ein Beispiel aus der Praxis: In einem grossen Treuhandbüro mit Hunderten Klienten wurde eine strikte Struktur für die digitale Ablage errichtet, in der auf jeden Ordner nur die für den jeweiligen Kunden zuständigen Treuhänder Zugriff hatten. Eine sichere Sache, könnte man meinen. Gleichzeitig wurden aber sämtliche Akten in gedruckter Form in einem Archivraum gelagert – und dieser war, mit einem einfachen Schloss gesichert, für mehr oder weniger jeden zugänglich, bis hin zum Reinigungspersonal.

Ein anderes Beispiel: Oft werden vorhandene Schutzmassnahmen, die etwa das Einstecken beliebiger USB-Datenträger unterbinden, aus Bequemlichkeitsgründen deaktiviert. Wenn der Faktor Mensch auf diese Weise zuschlägt, nützen die besten Tools wenig. Dies zeigt

deutlich, dass zu einer gelebten Zero-Trust-Kultur neben den technischen Massnahmen auch die Sensibilisierung der Mitarbeitenden gehört, die mit kontinuierlichen Security-Awareness-Schulungen erreicht werden kann.

Zero Trust ist also im Gesamten eine vielschichtige Angelegenheit, die weit ins Organisatorische hineinreicht, das gesamte zur Sicherung des Unternehmens erforderliche Ökosystem umfasst und gleichzeitig das herkömmliche Modell der Cybersecurity umkrempelt. Der Aufbau einer Zero-Trust-Architektur ist nicht trivial, aber er kann in Schritten erfolgen. Man kann mit einfachen Massnahmen beginnen, die sich mit vorhandenen oder neu ergänzten Sicherheitstools implementieren lassen. Neu ist die Zero-Trust-Idee übrigens nicht. Schon in den Urzeiten der Informatik wurde mit Black- und White-Listen gearbeitet, und damit wurden nur ausdrücklich genehmigte Verbindungen zugelassen – bis heute ein wichtiges Element der Cybersecurity.



Zero Trust umfasst – neben organisatorischen Aspekten – sämtliche Elemente der IT: von Netzwerk und Infrastruktur bis hin zu Daten und Anwendungen. Quelle: Boll Engineering

Vier Prinzipien

Eine umfassende Zero-Trust-Lösung basiert auf vier Prinzipien: explizite Verifizierung, geringstmögliche Berechtigungen, die Annahme, dass ein Sicherheitsvorfall jederzeit vorkommen kann sowie ein umfassendes Inventar der vorhandenen Ressourcen.

1. Jede Zugriffsanfrage und die Ausführung von Anwendungen und Services müssen geprüft und genehmigt werden, und zwar immer, auch wenn sie unternehmensintern erfolgen. Dabei können technische Elemente wie konventionelle Firewalls, Web Application Firewalls, Identity-and-Access-Management-Plattformen (IAM), Privileged-Access-Management-Lösungen (PAM) oder entsprechende Cloud-Dienste helfen.
   Zur expliziten Verifizierung gehört zwingend eine starke Authentifizierung mithilfe kryptografischer Technologie: Das wichtigste Element jeder Sicherheitsarchitektur sind die Identifizierung und der Schutz der Identität der beteiligten Akteure, seien es Software oder Menschen. Für den Zugriff durch menschliche Nutzer bedeutet dies unter anderem starke Passwörter oder vergleichbare Mechanismen sowie Mehrfaktor-Authentifizierung über Smartphone-Apps, physische Tokens oder biometrische Verfahren. Kaum jemand kann sich heute den Zugriff aufs E-Banking ohne solche Absicherung vorstellen, und mindestens das gleiche Sicherheitsniveau sollte auch fürs Firmennetz gelten.
2. Einmal grundsätzlich erteilt, darf der Zugriff nur auf diejenigen Ressourcen möglich sein, die für eine Aufgabe wirklich benötigt werden. Nicht jeder Nutzer braucht zum Beispiel Zugang zu einem ganzen Fileshare, wie es in der Vergangenheit oft gehandhabt wurde. Abgelegte Daten sollten klassifiziert und der Zugriff auf Basis der Klassifizierung individuell gewährt werden, wenn nötig bis auf die Ebene einzelner Dokumente. Analoges gilt für Anwendungen und (Micro-)Services. Auch solche teils automatisiert ablaufende Prozesse sollten nicht beliebig auf gespeicherte Daten und auch nicht auf den gesamten Arbeitsspeicher zugreifen dürfen. Moderne Lösungen können den gewährten Zugriff auf Ressourcen jederzeit und automatisiert wieder entziehen, sollte sich beispielsweise der Status des Endgerätes geändert haben (Risk-Adaptive Access Control).
3. Mit dem ständigen Bewusstsein, dass ein Breach womöglich schon passiert ist, fährt man grundsätzlich auf der sicheren Seite. Denn dann ist klar, dass jede Aktivität inspiziert und überwacht werden muss, und dies wiederum bedingt vollständige Visibilität über alle Aktivitäten und kontinuierliches Schwachstellenmanagement sowie Bedrohungserkennung und -abwehr. Auch dafür bietet der Markt Lösungen, oft cloudbasiert, wie etwa EDR (Endpoint Detection and Response) und XDR (Extended Detection and Response) im Bereich des Endpunktschutzes, Netzwerk-Monitoring-Plattformen sowie Firewalls, die auch den verschlüsselten Datenverkehr überwachen können. Solche Lösungen zählen eigentlich nicht direkt zu den Zero-Trust-Angeboten, unterstützen aber den Zero-Trust-Ansatz zusätzlich.
4. Auch das vierte Prinzip beschränkt sich nicht auf Zero-Trust-Umgebungen, sondern sollte Bestandteil jeder Sicherheitsstrategie sein und ganz am Anfang stehen: ein vollständiges, stets aktuelles Inventar aller relevanten Systeme, Anwendungen, Cloud-Dienste, Nutzer und Berechtigungen. Die dadurch erreichte Visibilität erleichtert die Einteilung der Ressourcen in einzelne Teilbereiche. So wird zum Beispiel Microsoft 365 samt seinen Anwendern zum eigenen Segment im Zero-Trust-Gesamtkonzept.

Mehr oder weniger komplex und aufwendig

Aus den erwähnten Lösungskategorien geht hervor, dass Zero Trust, rein technisch betrachtet, eine Vielzahl von Software- und Hardwareplattformen umfassen kann und der kombinierte Einsatz verschiedener Elemente ein komplexes Unterfangen darstellt. Es gibt Anbieter,

DIE AUTOREN

Peter Bernold ist Product Manager bei Boll Engineering und in dieser Funktion hauptsächlich verantwortlich für die Produkte und Lösungen von Palo Alto Networks. Der Security-Spezialist arbeitet seit 2015 für Boll.

Jürg Hefel ist bei Boll Engineering Product Manager für das IT-Security-Portfolio von Watchguard sowie für Endpoint-Security-Lösungen. Er ist seit über 35 Jahren in der IT-Branche tätig.

Ruedi Kubli ist seit 2020 Leiter des Fortinet-Teams bei Boll Engineering. Er ist seit über 30 Jahren im IT-Business tätig, stets mit Fokus auf Netzwerk- und IT-Security-Lösungen.

Boll Engineering zählt zu den führenden Schweizer Value-Add-Distributoren im Bereich IT-Security und vertreibtLösungen in den Bereichen Netzwerk- und Endpunktsicherheit, Cloud Native und SOC Security, Identity und Access Security, Vulnerability Management sowie Penetration Testing und E-Mail-Security. Das Unternehmen zählt rund 65 Mitarbeitende und hat seinen Hauptsitz in Wettingen.

die sämtliche Kategorien abdecken und ihre Produkte als integrierte Plattform verkaufen. Andere Hersteller fokussieren sich auf einzelne Kategorien und überlassen es den Unternehmen beziehungsweise deren Partnern, aus verschiedenen Lösungen nach dem Best-of-Breed-Prinzip eine Zero-Trust-Strategie umzusetzen. In beiden Fällen bringt eine erfolgreiche Transformation einiges an Aufwand mit sich – von der Evaluation der geeignetsten Lösung über die Implementierung bis zum laufenden Management, ganz zu schweigen von der Identifikation der Risiken und der Zuteilung der Berechtigungen.

Zero Trust im KMU

Das bedeutet aber keineswegs, dass Zero Trust im KMU nichts zu suchen hat, ganz im Gegenteil. Denn wie bereits erwähnt: Angesichts der Bedrohungslage kommt niemand mehr darum herum, mit dem impliziten Vertrauen aufzuräumen. Da kommt es gelegen, dass man – wie erwähnt – mit kleinen Schritten anfangen kann. Zum Beispiel mit einer Endpunktschutzlösung, die grundsätzlich auf Zero Trust setzt, ergänzt durch Zwei-Faktor-Authentifizierung, und so zumindest den Zugriff durch Mitarbeitende von ihren Geräten aus wasserdicht absichert.

Später lässt sich vielleicht eine Netzwerkmonitoring- oder Detection-and-Response-Lösung nachrüsten respektive ein entsprechender Managed Service einkaufen. So kann ein kompetenter Partner auch gleich die Analyse des Netzwerkverkehrs beziehungsweise die Bewertung und Abwehr von Bedrohungen oder die Reaktion auf Sicherheitsvorfälle, also das Incident Management, übernehmen. Das macht die Beschäftigung eigener, auf dem Arbeitsmarkt aktuell extrem schwer zu findender Security-Spezialisten überflüssig.

Aber es entbindet auch den kleinen Handwerksbetrieb nicht davon, sich über die Risiken Gedanken zu machen, die Bedeutung seiner Daten und Systeme zu analysieren und das Netzwerk sinnvoll zu segmentieren (muss die vernetzte CNC-Maschine wirklich im gleichen Netzwerkteil untergebracht sein wie der Buchhaltungs-PC?). Und wenn man schon dabei ist: Warum nicht gleich Software, Daten und Geräte ausmisten, die seit Jahren herumstehen, aber nicht mehr wirklich gebraucht werden? Solche Altlasten sind oft mangelhaft gesichert und bergen erhebliche Risiken.

Das Fazit: Zero Trust ist ein Transformationsprozess, der Zeit und Ressourcen bindet, also nicht einfach so funktioniert. Der Zero-Trust-Ansatz lässt sich schrittweise umsetzen, beginnend mit einem soliden Konzept, einem Inventar der vorhandenen Ressourcen und Identitäts- und striktem Zugriffsmanagement für menschliche Nutzer samt Mehrfaktor-Authentifizierung. ■