STORMSHIELD

MEINUNGEN

ZERO TRUST NETWORK: SOLLTEN SIE (WIRKLICH) VERTRAUEN IN NICHTS HABEN?

Sébastien Viou
Cybersecurity Product Director & Cyber-Evangelist, Stormshield

Das Zero-Trust-Modell ist en vogue. Und es bringt ein einfaches Versprechen mit sich: Um Ihr IT-System vor Cyber-Bedrohungen zu schützen, müssen Sie alles anzweifeln und Vertrauen in nichts haben. Was wäre, wenn es nicht darum ginge, Vertrauen abzuschaffen, sondern es zu verschieben?

Die Unternehmensnetzwerkumgebung ist tot, es lebe das Zero Trust Network? Das von Forrester in den späten 2000er Jahren vorangetriebene Sicherheitsmodell „Zero Trust Network Access" (abgekürzt *Zero Trust Network* oder auch *Zero Trust*) wird heute regelmäßig propagiert, um mit Cyber-Bedrohungen und dem prognostizierten Verschwinden der Unternehmensnetzwerkumgebung umzugehen. Es ist jedoch von grundlegender Bedeutung, sich daran zu erinnern, dass **ZTN keine Technologie ist, sondern eher ein Ansatz, fast eine Philosophie, die unser Vertrauensverhältnis in Frage stellt und ein Sicherheitsmodell mit verschiedenen technologischen Bausteinen aufbaut**. Ein Blick hinter die Kulissen des Zero-Trust-Ansatzes.

DIE NETZWERKUMGEBUNG VERSCHWINDET

Vor langer Zeit gab es eine rote Linie zwischen dem, was sich innerhalb des Firmennetzwerks befand und daher als vertrauenswürdig galt, und dem, was sich außerhalb befand und daher als potenzielle Bedrohung wahrgenommen wurde. Dieser Ansatz bot eine Form von physischer Sicherheit, bei der das Netzwerk nur in den Räumlichkeiten des Unternehmens zugänglich war. Und ohne Zugang zu den Räumlichkeiten gibt es auch keinen Zugriff auf das Netzwerk - außer über einen VPN-Zugang. Einfach, grundlegend.

Doch die digitale Transformation hat die Architektur der Systeme tiefgreifend verändert. Von der weit verbreiteten Nutzung von VPN-Zugängen zur Absicherung von Fernarbeit bis hin zu Cloud-Anwendungen und -Infrastrukturen ist die Unternehmensnetzwerkumgebung heute buchstäblich fragmentiert. So sehr, dass es nicht mehr viel Sinn ergibt, den Schutz des Unternehmens auf seine Netzwerkumgebung zu beschränken.

KOPFZERBRECHEN BEI DER SICHERUNG DES FERNZUGRIFFS

Neben dem Aufkommen der Cloud und dem weit verbreiteten Einsatz von Telearbeit führt der Trend „*Bring Your Own Device*“ zu einem Ende der Unternehmensnetzwerkumgebung und wirft neue Sicherheitseinschränkungen auf. Mit zwei klassischen Prioritäten für die Sicherung von Fernzugriffen: **Benutzer zu authentifizieren und zu autorisieren.**

Der erste Punkt kann (zum Teil) mit dem VPN angegangen werden. Durch die Schaffung eines sicheren und verschlüsselten Zugangstunnels ermöglicht das Unternehmen dem Mitarbeiter auf Unternehmensressourcen zuzugreifen, unabhängig davon wo sie sich befinden, und Daten sicher zu übertragen. Damit delegiert das Unternehmen sein Vertrauen an den VPN, was viele Vorteile hat: ein gut beherrschtes Protokoll, bekannte Verschlüsselungsalgorithmen und verwendete Schlüsselgrößen sowie gut identifizierte Kapazitäten und Grenzen. Die Identifizierung und Authentifizierung werden scheinbar von Tools für die Fernverbindung und 2FA-Lösungen übernommen. Aber es gab immer noch das Problem der Zugangskontrolle für heterogene Anwendungen und unkontrollierte Geräte. Daher das Aufkommen des Zero-Trust-Ansatzes in den letzten Jahren.

ZERO TRUST ODER DIE ZENTRALE FRAGE DES VERTRAUENS

Im Gegensatz zu VPN, das Vertrauen in eine sichere Verbindung zwischen zwei Entitäten herstellt, geht es beim Zero-Trust-Ansatz um das Vertrauen in... nichts. Bei diesem Ansatz wird daher das Netzwerk befragt, um zu kontrollieren, wer wann auf was zugreift. Mit anderen Worten: Der Zero-Trust-Ansatz basiert auf der Überprüfung von Zugängen, Identitäten und Berechtigungen an jedem Zugangspunkt - auch innerhalb des Unternehmensnetzwerks. „*Das ZTN verspricht Null Vertrauen*“, sagt **Stéphane Prévost**,

Product Marketing Manager bei Stormshield. *„Aber das ist unmöglich! Man muss sich an etwas Greifbarem festhalten, um Zugang zu etwas Vertraulichem geben zu können.*" Oder anders gesagt: Wie viel Vertrauen muss je nach Vertraulichkeit der zu schützenden Informationen oder Umgebung gegeben werden?

„Das ZTN verspricht Null Vertrauen, aber das ist unmöglich! Man muss sich an etwas Greifbarem festhalten, um Zugang zu etwas Sensiblem geben zu können."

Stéphane Prévost, Product Marketing Manager bei Stormshield

Beim ZTN-Ansatz geht es nicht darum, Vertrauen abzuschaffen, sondern es zu verschieben. Wohin? Zunächst einmal zum Benutzer. Mit einem einfachen Prinzip: Wenn der Benutzer authentifiziert ist, kann ich ihm vertrauen. Aber ist das wirklich genug? Was ist mit seinem Standort oder seinem Anschlussgerät?

EIN DREI-PUNKTE-SICHERHEITSFUNDAMENT: IDENTITÄT, GERÄT UND ZUGRIFF

Neben den beiden bereits erwähnten traditionellen Prioritäten gibt es in der Tat eine dritte. Der Benutzer ist zwar zentral, aber auch das Gerät, das er benutzt, ist wichtig. *„Es ist die Kombination von Benutzer und Gerät, die beim Zero-Trust-Ansatz wichtig ist*", erklärt Stéphane Prévost. *„Selbst wenn Sie einen Benutzer authentifizieren, besteht immer noch eine mögliche Sicherheitslücke auf dem verwendeten Gerät. Es kann mit einem Virus infiziert werden, der z. B. auf vertrauliche Inhalte zugreifen und Daten verschlüsseln kann. Wir müssen also auch dem Gerät vertrauen.*" Und die Zugänge je nach Art des Arbeitsplatzes (beruflich oder privat), der verwendeten Softwares, der Aktualisierung seiner Sicherheitslösungen oder sogar des Ortes, an dem er sich befindet (zu Hause, im Büro, unterwegs usw.) verwalten. Damit dies möglich ist, **müssen Schutzlösungen für Arbeitsplätze kontextbezogene Richtlinien und die dynamische Anpassungsfähigkeit einbeziehen**. Und damit die Sicherheit an die Umgebung anpassen.

„Es ist die Kombination von Benutzer und Gerät, die beim Zero-Trust-Ansatz wichtig ist."

Stéphane Prévost, Product Marketing Manager bei Stormshield

Beim Zero-Trust-Ansatz geht es nicht nur um den Zugang zum Unternehmensnetzwerk, sondern um eine umfassende, personen- und gerätebezogene Sicherheit, die Benutzer- und Geräteidentifikation, Multi-Faktor-Authentifizierung und Zugriffsmanagement umfasst.

Dieser letzte Punkt setzt **eine gewisse Reife der Unternehmen in diesem Bereich** voraus, insbesondere um die Zugriffsrechte der einzelnen Mitarbeiter klar zu definieren. Und genau da liegt manchmal das Problem. Denn das Identitäts- und Zugangsmanagement

(*Identity and Access Management* - IAM) liegt nicht nur in der Verantwortung der IT-Abteilung. Die Personalabteilung sowie die Verantwortlichen der einzelnen Abteilungen oder Geschäftsbereiche müssen eine klare Vorstellung von den gewährten Zugängen haben. Jeder Manager muss in der Lage sein, zu bestimmen, wer in seinem Team Zugriff auf was hat und wer was tun darf. Es hört sich einfach an, aber im Verhältnis zu der wachsenden Anzahl an Tools in einem Unternehmen kann die fließende Verwaltung aller Berechtigungen und ihrer Aktualisierungen schnell zu einem Kraftakt werden. Aber es ist ein notwendiges Projekt, das zur Sicherheit des Unternehmens beiträgt. Die gute Nachricht ist, dass die Implementierung schnell geht, wenn die Arbeit erst einmal getan ist. Die schlechte Nachricht ist, dass Unternehmen mit einer sich im Laufe der Zeit entwickelnden Richtlinie und einer starken Heterogenität der Überwachungstools umgehen müssen, um die Kontrolle zu behalten und einen umfassenden Überblick über den Zugriff zu haben, insbesondere wenn ihre Anwendungen in einer Cloud gehostet werden.

DIE BESONDERHEIT VON CLOUD-MODELLEN

Ob IaaS- oder PaaS-Infrastrukturen, SaaS-Anwendungen oder auch hybride Infrastrukturen: Die Nutzung der Cloud explodiert in Unternehmen. So lagern 51 % der befragten französischen Organisationen und Unternehmen ihr Informationssystem ganz oder teilweise und 7 % sogar vollständig an einen Dritten aus, stellt Clusif in der Ausgabe 2020 der MIPS-Studie (Computerbedrohungen und Sicherheitspraktiken) fest.

Unternehmen migrieren ihre eigenen benutzerdefinierten Anwendungen in die Cloud und/oder abonnieren SaaS-Unternehmensanwendungen wie Office 365, Salesforce, Google oder andere. Allerdings hat eine aktuelle ESG-Umfrage ergeben, dass Konten und Rollen mit zu freizügigen Berechtigungen die Nummer eins bei der Fehlkonfiguration von Cloud-Diensten sind. Die Definition einer Least-Privilege-Zugriffsrichtlinie ist daher in einer Cloud-Umgebung unerlässlich... aber komplex. „*Das Unternehmen muss in der Lage sein, die Person zu identifizieren, die sich mit diesen verschiedenen Anwendungen verbindet*“, erklärt Stéphane Prévost. Das Unternehmen sieht sich dann mit verschiedenen technischen Bausteinen und einer sehr heterogenen Zugriffsrichtlinie, die es zu verwalten gilt, konfrontiert: die Richtlinie für das Rechenzentrum, die Richtlinie für Remote-Standorte, die Richtlinie für SaaS- und PaaS-Anwendungen usw.

„*Es ist kompliziert, die Vollständigkeit des Zugriffs zu verarbeiten*“, sagt Stéphane Prévost. „*Die Unternehmen haben noch keine einzelne Richtlinie, die in der Lage ist, die Rechte für den Zugang von wem auf was und wann bereitzustellen! Dies wird sich aber sicherlich auf das Firmenverzeichnis stützen.*“

Ein Verzeichnis als zentraler Punkt des Identitätsmanagements in einem Unternehmen. Das ist ein Thema, das die Frage nach einer gewissen Abhängigkeit von seinem Herausgeber aufwirft. Und das selbst dann, wenn es durch IAM-Lösungen verstärkt werden kann. Rollen, die auf Benutzer angewendet werden, erfordern viele Genehmigungen, die am besten auf die geringste Menge an Berechtigungen beschränkt werden, die für die Funktion eines bestimmten Dienstes erforderlich sind. Ein weiterer Punkt, auf den Sie achten sollten, sind veraltete Berechtigungen, die den Zugriff von

Personen aufrechterhalten, die nicht mehr an dem Projekt arbeiten. Am einfachsten ist es, in Etappen vorzugehen: **Beginnen Sie mit einem Minimum an Berechtigungen und gewähren Sie dann bei Bedarf mehr**. Diese Methode ist sicherer, als mit zu freizügigen Berechtigungen zu beginnen und später zu versuchen, sie einzuschränken (Sie könnten einige vergessen).

Zusammenfassend lässt sich sagen, dass ein Zero-Trust-Ansatz mehrere Voraussetzungen erfordert:

- Kontrollieren Sie die Sicherheitsstufe von Arbeitsplätzen und Anwendungszugriffsgeräten;
- Definieren Sie, wer wie auf was zugreift (und stellen Sie diese Frage regelmäßig);
- Stellen Sie diese Zugriffsrichtlinie homogen auf allen Anwendungen bereit, die manchmal sehr heterogen sind.

EINE ÄNDERUNG DER PHILOSOPHIE

Durch die Verlagerung des Vertrauens auf die Identifizierung und Authentifizierung des Benutzers, seines Zugangs und seines Geräts macht **der Zero-Trust-Ansatz die Identität zu einem neuen Sicherheitsperimeter.** Dies erfordert die Implementierung von Überprüfungsmechanismen in einem sehr frühen Stadium, nämlich auf der Ebene der Geschäftsanwendungen, die sich bisher ausschließlich auf die Netzwerkzugangskontrolle verlassen haben. „*Das hindert uns nicht daran, bewährte Praktiken rund um das ZTN zu implementieren, wie zum Beispiel die Segmentierung des Unternehmensnetzwerks nach dem Grad des Vertrauens, das den Mitarbeitern entgegengebracht wird*", betont Stéphane Prévost.

Es wäre in der Tat eine Illusion zu glauben, dass Zero Trust ein magischer Ansatz ist, der alle anderen Sicherheitsansätze ersetzt. Tatsächlich stützt er sich auf bestehende Technologien, um das richtige Maß an Vertrauen zu schaffen: Multi-Faktor-Authentifizierung, um dem Benutzer zu vertrauen, VPN, um die Kommunikation zu verschlüsseln und ihrer Übertragung zu vertrauen, Verhaltensanalyse, um dem verwendeten Gerät zu vertrauen usw. Der Fokus liegt auf der kontinuierlichen Neubewertung des zu gewährenden Vertrauensgrades. Dies bestätigt ein unveränderliches Prinzip: Cybersecurity ist kein statischer Bereich, sondern eine kontinuierliche Entwicklung.