Zero Trust: gar nicht so viel Zauber wie man denkt

Zero Trust ist von Mythen umgeben wie der Heilige Gral. Aber was ist belegbar und welche Haltung wird kultiviert? Und welche Vor- und Nachteile hat diese Security-Philosophie für Unternehmen? Sophos hat sich das Prinzip des „Traue niemandem, verifiziere alles" genau angesehen und ein White Paper zur Orientierung herausgegeben.

Das Zeitalter von Corporate Networking und einzelnen, abgekoppelten Netzwerken ist endlich. Nutzer arbeiten – und das nicht nur zurzeit – immer mehr von Zuhause und benötigen dafür nur das öffentliche Netz. Die Verlässlichkeit sämtlicher genutzter Systeme ist allerdings unabdingbar. Der Umgang damit kann aber auch zur Haltungsfrage werden. Und genau hier schlägt die Stunde der Zero-Trust-Security-Philosophie: Das Prinzip fußt auf der Idee: vertraue niemandem, überprüfe alles. Was der Annahme von Verlässlichkeit grundlegend widerspricht. Im Fokus steht der ausnahmslose Schutz der Ressourcen, egal ob physisch oder digital. Nichts ist vertrauenswürdig. Niemals.

Große Idee mit vielen Vorteilen
Der Einsatz einer Zero-Trust-Security-Philosophie im Unternehmen bringt zahllose Vorteile mit sich, besonders aber den Überblick über den gesamten IT-Kosmos, bis hin zum einzelnen Remote-Arbeitsplatz. Drei entscheidende Gedanken prägen Zero Trust dabei:

- Es gibt kein „Innerhalb" im Netzwerk, also das Bewusstsein, dass man sich trotz übergeordnetem Netzwerk dennoch selbst schützen muss.
- Jedes System im inneren wie äußeren Netzwerk kann jederzeit angegriffen werden.
- Sicherheitsmaßnahmen müssen dynamisch und in Echtzeit sein.

Modus Operandi: Identifizieren – Kontrollieren – Analysieren – Sichern
Wer niemandem traut, ist gezwungen, sich um eigene Sicherheitsmaßnahmen für seine gefährdeten Bereiche zu kümmern. Insofern führt Zero Trust zu diesen vier Handlungsprinzipien:

- Identifizierung eines jeden Users mit multiplen Faktoren.
- Zugangskontrolle: Nutzer sollten nur Zugang zu den Bereichen haben, die sie benötigen
- Analyse sämtlicher Netzwerk- und Systemaktivitäten, um rechtzeitig Unregelmäßigkeiten zu erkennen, nützlich sind hier ERD, SIEMs und MDR.
- Sichern von innen heraus: was sind die wichtigsten Daten, welche möglichen Verletzbarkeiten existieren auf dem Weg dieser von Innen über das Netzwerk zum Adressaten.

Das Zero-Trust-Prinzip ist mitunter sperrig und mühsam, bietet aber auch viele Vorteile. Da sich auch die Cyberkriminalität sehr kreativ weiterentwickelt, ist diese Grundhaltung eine Möglichkeit, die Bedrohungslage wirklich zu minimieren, in dem man quasi alles per se für unsicher hält. Zeitgleich ist das aber auch eine Aufforderung, neue Standards im Cybersicherheitsprotokoll zu entwickeln.

Detaillierter Ausführungen zu Zero Trust hat Sophos im einem englischen Whitepaper hier zusammengefasst.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de