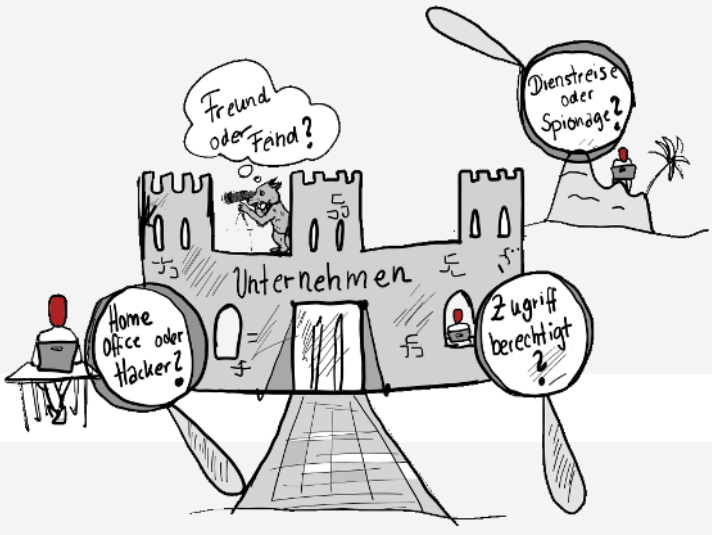
synalis

Cloud für den Mittelstand von morgen.

Volle Kontrolle über Netzwerkzugriffe

Zero Trust Protection



Zero Trust auf einen Blick

Konzeptionelles Sicherheitskonzept, das informationsbasierten Zugriffsanalysen und –regelungen folgt

Erprobter Ansatz, um weitreichenden Schaden durch **unkontrollierten Zugriffsmissbrauch** auf das gesamte Unternehmensnetzwerk zu verhindern (etwa durch einen Hackerzugriff, nachdem Kriminellen mit einem Schlag alle Türen offen stehen)

Bislang verbreiteter **Level of Trust** / unternehmensweiter Netzwerkzugriff wird zeitgemäß **überholt** zugunsten verstärkter Unternehmenssicherheit

Optimierung des Identitäts- und **Zugriffsmanagements**

Konstante Auswertung bei Logins (Zugriffsort, Zugriffsgerät, Risikobewertung des Nutzers)

Hohe Differenzierung & **Mikro-Segmentierung** bei Zugriffsrechten, sowohl bei Applikationen als auch privilegierten Benutzern

Vorgang nach dem **Minimalprinzip**: So viele Rechte wie nötig, so wenig wie möglich zur Reduktion von Angriffsflächen

Vertrauen ist gut, Kontrolle besser

Ein solider Lösungsansatz, um sich auch in der heutigen IT-Welt vor Angriffen schützen zu können, bietet das Zero Trust Model. Es folgt dem Motto „**Never trust, always verify**“ – ohne Einschränkungen in Mobilität und Funktion.

Mit dem Zero.Trust-Ansatz formt sich ein **Paradigmenwechsel** zu herkömmlichen Security-Konzepten, die die Überwachung des eigenen Netzwerkes nicht immer implizieren:

Zero Trust hingegen umfasst auch die Auswertung netzwerkinterner Geräte, Dienste und Anwender und erhöht somit den Schutz.

Ihr Ansprechpartner

Daniel Philips
Head of CIS

Telefon: +49 228 9268 121
E-Mail: **daniel.philips@synalis.de**

synalis

Cloud für den Mittelstand von morgen.

Eine Frage der Sicherheit:

Zero Trust Protection

Auf Nummer sicher gehen

So werden beispielsweise sämtliche Zugriffe abgesichert und differenzierte Bedingungen eines jeden Logins hinzugezogen sowie bewertet.

Findet etwa zu außergewöhnlichen Zeiten ein Anmeldeversuch aus dem Ausland statt, obwohl dort keine Kollegen vertreten und Niederlassungen verortet sind, ist die interne IT schnell informiert und alarmiert.

Verdachtsfälle werden rasch klassifiziert und führen zu einer deutlichen Erhöhung Ihrer Unternehmenssicherheit:

Clouddienste, mobile Arbeit und Homeoffice sind spätestens seit Corona ein Muss und ermöglichen volle Flexibilität. Auf der anderen Seite geht damit eine fortschreitende **Dezentralisierung von Daten und Zugriffen** einher und eröffnet Hackern neue Einfallstore.

Daher erfordert die IT-Sicherheit nun ein besonderes Augenmerk.

Application Access ≠ Network Access

Daten und Systeme werden im Rahmen des Zero Trust Models konstant und ausnahmslos klassifiziert und eine sogenannte **Mikro-Segmentierung** durchgeführt, um alle Logins kritisch zu betrachten und verlässlich auszuwerten. Jede Anmeldung stellt eine komplexe Kombination von Kriterien dar, die automatisch analysiert werden.

Durch eine **erfolgreiche Authentifizierung** im Netzwerk hat der Mitarbeiter daher **nicht zwingend vollständigen Datenzugriff**. Erst die Beurteilung aller Signale entscheidet über die der Nutzerrolle angepassten **Zugriffsrechte**.

Das Zero Trust Model schützt längst nicht nur die hier beispielhaft aufgeführten Anmeldeprozesse: Als **holistisches Sicherheitskonzept** sollte es die Grundlage sämtlicher Unternehmensprozesse sein, die Sicherheitsrisiken bergen können.

IT-Sicherheit und Cyber Security sind auch für Sie ein Thema: