E-BOOK

Mehr Sicherheit für Unternehmen: **12 Tipps** für Ihre IT-Sicherheitsstrategie nach Zero Trust

www.orbit.de

ORBIT IT-SOLUTIONS

Inhalt

01. Was bedeutet Zero Trust?

Zero Trust ist ein IT-Sicherheitskonzept für Unternehmen, das John Kindervag schon im Jahr 2010 als Vizepräsident und Chefanalyst von Forrester Research geprägt hat. Nach Zero Trust wird grundsätzlich allen Geräten, Anwender*innen und Diensten misstraut und der Zugriff auf Ressourcen erst nach eingehender Überprüfung und Authentifizierung zugelassen. Auf diese Weise werden Sicherheitsrisiken von außen und innen minimiert.

Hacker-Angriffe werden immer präsenter, die Nachrichten über betroffene Unternehmen häufen sich. Tatsache ist: Die Digitalisierung treibt nicht nur den Einsatz von Cloud-Infrastrukturen voran und sorgt für einen Wandel der Arbeitswelt hin zu mobilem Arbeiten, sondern begünstigt gerade dadurch auch Lücken in der Abwehr eines Unternehmens und die Zunahme von Angriffsflächen.

Die IT-Sicherheit muss folglich der veränderten Infrastruktur angepasst werden und berücksichtigen, dass beispielsweise durch mobiles Arbeiten Zugriffe auf Unternehmensdaten nicht mehr nur innerhalb des eigenen Netzwerks passieren, sondern von überall. Der Ansatz, nichts und niemandem zu vertrauen, setzt genau dort an, gewährleistet eine kontinuierliche Verifizierung aller Transaktionen und sorgt durch automatisierte Echtzeiterkennung sowie -reaktion auf Bedrohungen für die Sicherheit digitaler Daten.

Um vollumfänglichen Schutz bieten zu können, baut Zero Trust auf 6 Säulen auf:

1. Identity
Authentifizierung von Identitäten und Zugriffen

2. Endpoint
Schutz von Endgeräten und Prüfung der Integrität

3. Apps
Überprüfung und Eingrenzung von Berechtigungen und Zugriffen auf Anwendungen

4. Network
Netzwerksegmentierung zur Verhinderung von unbefugten Zugriffen und anderen Bedrohungen im Netz

5. Infrastructure
Auswertung von Telemetriedaten in Echtzeit und deren Nutzung für automatische Aktionen

6. Data
Klassifizierung und Schutz von Daten sowie Verschlüsselung des Datenverkehrs

Das Zero-Trust-Konzept ist nachvollziehbar und klingt vielversprechend.
Der nächste Schritt wäre also: Umsetzen! Oder? Und vor allem: Wie?

02. Die Komplexität von Zero Trust anhand eines Beispiels

Ganz so einfach mit der Umsetzung bzw. Einrichtung einer Zero-Trust-Architektur – nach dem Motto „Einfach machen!" – ist es dann leider nicht. Der Zero-Trust-Ansatz ist nicht nur umfassend, sondern auch sehr komplex, sodass er sich nicht mal eben mit 3 Klicks umsetzen lässt. Wie komplex das Sicherheitsprinzip ist, veranschaulicht folgendes Negativ-Szenario, bei dem keinerlei Schutzmaßnahmen zum Einsatz kommen:

Was wäre, wenn … Ein CEO einer Firma ist auf Geschäftsreise und bei seinem Aufenthalt am Bahnhof möchte er die Zeit nutzen, um in seine geschäftlichen E-Mails zu schauen. Er greift also mit seinem mobilen Endgerät von unterwegs auf seine E-Mails zu. Das Gerät baut folglich über ein öffentliches Netzwerk eine Verbindung zur Firmen-Domain auf, klassisch: exchange.kunde.de.

Auf diese Weise bekommt ein Hacker, der sich mit einem Sniffer und/oder eigener Funkzelle vorbereitet oder sich schon Zugang zum öffentlichen HotSpot verschafft hat, mit, welches Gerät mit der Firmen-Domain interagiert und auf welches Gerät er sich zu dem Zeitpunkt konzentrieren muss, um gezielt den Netzwerkverkehr mitzuschneiden. Er kennt nun also die Firmen-Domain, das Unternehmen und die E-Mail-Adresse des Users. Das erleichtert ihm die Identifizierung der User-Identität, um erfolgreich angreifen zu können. Ein CEO steht außerdem in der Öffentlichkeit, sodass auch schnell der User selbst bekannt ist. Dadurch wiederum hat der Hacker leichtes Spiel, sobald der CEO sich bei irgendeinem anderen Dienst mit seinem Passwort authentifiziert. Dann ist der Weg frei, der Hacker kann die Identität des CEO übernehmen und mit der gestohlenen Identität auf sämtliche Unternehmensdaten zugreifen. Selbst wenn der CEO sich nicht bei einem anderen Dienst anmelden würde, könnte der Hacker über Social Engineering weitere Informationen und somit Daten über ihn herausfinden (hat er einen Hund, bestimmtes Hobby, Kinder, soziale Kontakte etc.) und über Versuch und Irrtum oder mit Tool-Unterstützung das Passwort ermitteln und hätte Zugang zu allen Daten.

Was hat letztlich dazu geführt, dass der Hacker leichtes Spiel für den Identitäts- und Datendiebstahl hatte?

1. Das Endgerät und die Identität des CEO waren nicht gesichert.
2. Die Verbindung zur Firmen-Domain war nicht verschlüsselt und die Identität sichtbar.
3. Das Netzwerk war nicht segmentiert und alle Daten zugänglich.

03. Vertrauen ist gut, Kontrolle ist besser!

Eine hundertprozentige Sicherheit gibt es nicht, denn dafür müssten Unternehmen alle eingesetzten technischen Mittel in der Tiefe kennen, jedes Verhalten ihrer User voraussehen und letztlich vollständig kontrollieren können.

Hierbei geht es aber schon um banale Dinge, wie das Umgehen der VPN-Nutzung, weil diese nicht ohne Hürden möglich ist oder die Geschwindigkeit der Internetverbindung drosselt. Auch das Nutzen eigens ausgewählter Tools als Hilfsmittel oder separate (Cloud-)Speicherorte steigern das Risiko für Datenpannen – Stichwort Schatten-IT. User-Verhalten bringt IT-Sicherheitsexpert*innen schnell an ihre Grenzen. Ganz ohne Vertrauen bzw. Sensibilisierung für den vorsichtigen Umgang mit Daten geht es also auch nicht.

Nach Zero Trust geht man davon aus, dass immer wenigstens 1 der 6 Säulen, auf denen der Sicherheitsansatz fußt – Identity, Endpoint, Data, Apps, Network und Infrastructure –, erfolgreich angegriffen wird. Auf diese Weise findet auf mehreren Ebenen – durch ein Zusammenspiel verschiedener Technologien und Prozesse – die Absicherung des Unternehmens und seiner digitalen Daten statt für einen verbesserten Schutz.

Unternehmen erreichen folglich mit der Implementierung einer Zero-Trust-Architektur mehr Sicherheit bei weniger Risiken. Durch die Auseinandersetzung mit einem neuen Sicherheitsmodell trägt Zero Trust außerdem dazu bei, das Sicherheitsbewusstsein einer Organisation nachhaltig zu schärfen.

Gerade, weil die Risiken für Unternehmen durch diverse Faktoren – egal ob aggressive Hacker oder arglose Mitarbeiter*innen – steigen, ist der Umstieg auf einen modernen und vor allem proaktiven Sicherheitsansatz wie Zero Trust umso wichtiger.

12 TIPPS: SO SCHÜTZEN SIE IHR UNTERNEHMEN NACH ZERO TRUST

1. Verwenden Sie Multifaktor-Authentifizierung (MFA)

MFA ist eine wichtige Komponente von Zero Trust. Benutzer*innen sollten mindestens zwei Faktoren zur Authentifizierung verwenden müssen, um Zugriff auf Ressourcen zu erhalten.

2. Implementieren Sie Zugriffskontrollen

Verwenden Sie Zugriffskontrollen, um den Zugriff auf Ressourcen zu kontrollieren und sicherzustellen, dass nur berechtigte Benutzer*innen und Geräte Zugriff haben.

3. Identifizieren Sie wichtige Assets

Identifizieren Sie Ihre wichtigen Systeme, Daten und Anwendungen und definieren Sie Zugriffsrichtlinien basierend auf den Identitäten der Benutzer*innen, Geräte und Anwendungen.

4. Beschränken Sie den Zugriff auf das notwendige Minimum

Vergeben Sie nur die Zugriffsberechtigungen, die unbedingt notwendig sind für Benutzer*innen und Geräte, um ihre Arbeit zu erledigen.

5. Sorgen Sie für sichere Geräte

Überprüfen und gewährleisten Sie, dass alle Geräte, einschließlich IoT- und mobile Geräte, sicher sind und alle Sicherheitsanforderungen erfüllen.

6. Überwachen Sie den Datenverkehr

Überwachen Sie den Datenverkehr in Echtzeit, um verdächtige Aktivitäten zu erkennen, zu analysieren und darauf zu reagieren.

7. Verschlüsseln Sie alle Daten

Sorgen Sie dafür, dass alle Daten verschlüsselt werden, sowohl im Ruhezustand als auch während der Übertragung, um sicherzustellen, dass sie vor unbefugtem Zugriff geschützt sind.

8. Verwenden Sie Mikrosegmentierung

Teilen Sie Ihr Netzwerk in kleine, isolierte Segmente auf, um die Angriffsfläche zu reduzieren und die Auswirkungen von Angriffen zu begrenzen.

9. Implementieren Sie einen Zugriffsverweigerungsmechanismus

Um sicherzustellen, dass unautorisierte Benutzer*innen und Geräte vom Netzwerk ferngehalten werden, benötigen Sie einen Mechanismus zur Verweigerung des Zugriffs.

10. Überprüfen und aktualisieren Sie regelmäßig

Überprüfen und aktualisieren Sie Ihre Sicherheitsrichtlinien und -maßnahmen regelmäßig, um sicherzustellen, dass sie den aktuellen Bedrohungen und Risiken entsprechen.

11. Verschleiern Sie Ihre Identitäten

Verschleiern Sie mittelfristig alle Identitäten in Ihrem Unternehmen, indem Sie ausschließlich nicht identifizierbare Einstiegspunkte in Ihre Infrastruktur nutzen.

12. Schulen Sie Ihre Kolleg*innen:

Schulen Sie Ihre Kolleg*innen in Bezug auf Cybersicherheit und die Bedeutung der Einhaltung von Sicherheitsrichtlinien.

Diese Tipps können Ihnen helfen, ein effektives Zero-Trust-Sicherheitskonzept zu implementieren und Ihr Netzwerk vor Bedrohungen zu schützen.

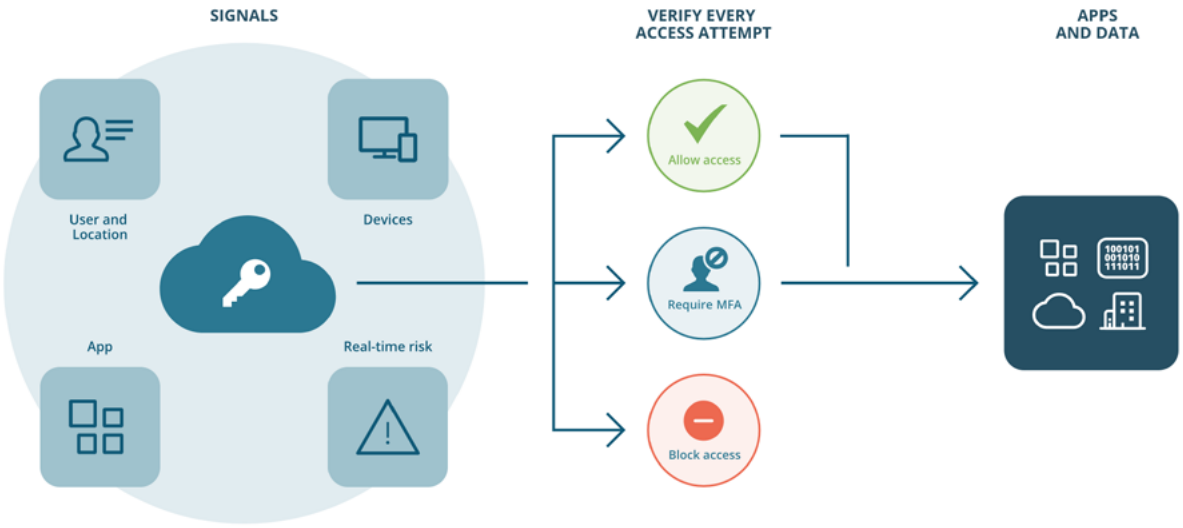
www.orbit.de

ORBIT IT-SOLUTIONS

05. Ohne Sicherheitsstrategie geht es nicht

Doch bevor Sie sich in Ihrem Unternehmen in die Umsetzung stürzen, bedarf es einer umfassenden Sicherheitsstrategie, in die Sie den Zero-Trust-Ansatz einbetten. Denn nur wenn Zero Trust Teil eines IT-Sicherheitsgesamtkonzepts ist, das die 6 Zero-Trust-Säulen Identity, Endpoint, Data, Apps, Network und Infrastructure in Einklang bringt, kann es funktionieren.

So können Sie Ihr Unternehmen gut absichern und Ihre vertraulichen Daten schützen.



Diese vereinfachte Grafik zeigt, wie der Sicherheitsansatz nach Zero Trust funktioniert, welche Faktoren und Vorgänge zum Tragen kommen.

06. Change Management für den Erfolg Ihrer Sicherheitsstrategie

Die Implementierung von Zero Trust bringt Veränderungen mit sich, die auch Ihre Kolleg*innen betreffen:

Gerätenutzung
z. B. Regelung, ob und inwiefern Firmengeräte privat genutzt werden dürfen, welche Geräte das Unternehmen anbietet und ob die Nutzung von privaten Endgeräten erlaubt ist

Authentifizierungsverfahren
z. B. Zugangs- und Zugriffsregelung über Zugangskarten fürs Firmengebäude, 2. Faktor wie Token und/oder Smartphone; täglich teilautonome Anmeldung/Bestätigung der Identität

Änderung des Datenablageorts
z. B. Regelung für die Zusammenarbeit, u. a. was mit Externen geteilt werden darf und was nicht und welche Berechtigungen Externe sowie Gäste erhalten

WLAN-Verbindung nicht mehr über Passwort
Es kann nicht mehr jedes beliebige Gerät mit dem Unternehmens-WLAN verbunden werden

Automatische Authentifizierung
User müssen nicht mehr überall ein Passwort eingeben, wenn bestimmte Faktoren gegeben sind

Einschränkung von Zugriffs-, Nutzungs- und Bearbeitungsrechten
Just-In-Time (JIT) und Just-Enough-Access (JEA)

Cloud-Nutzung
z. B. befinden sich Clients nicht mehr im internen Netzwerk, sodass Mitarbeitende von überall arbeiten können

… um nur einige Beispiele zu nennen, die sich auf das gesamte Unternehmen auswirken.

Veränderungen werden in der Regel aber eher skeptisch, wenn nicht sogar ablehnend betrachtet, unabhängig davon, dass sie auch positive Auswirkungen auf den Arbeitsalltag haben können. Deshalb ist es unbedingt notwendig, dass Sie den Change von Anfang an kommunizieren, die Kolleg*innen über Ihre Pläne informieren und sie einbeziehen sowie den Nutzen für das Unternehmen darstellen.

Steigern Sie die Akzeptanz für Ihr Projekt, indem Sie

» alle Stakeholder identifizieren und abholen
» den Change als gemeinsames Ziel formulieren und ins Unternehmen tragen
» alle Schritte und Veränderungen transparent kommunizieren
» für alle Betroffenen Trainings- & Unterstützungskonzepte erstellen und umsetzen

Auf diese Weise sichern Sie Ihre Investition und erhalten Unterstützung für Ihr Vorhaben. Sicheres Arbeiten und geschützte Daten betreffen schließlich jede*n Einzelnen im Unternehmen. Ihre Kolleg*innen werden bald die Vorteile des neuen Sicherheitskonzeptes erkennen:

Verbesserung der Usability für jede*n Einzelnen

» geschützter Zugriff von überall über digitale Anwendungen
» sicherer und erleichterter Wechsel zwischen Remote- und Büroarbeit
» positives Nutzererlebnis durch Single Sign-on, Wegfall von zwingender Nutzung des Unternehmensnetzwerks (z. B. über VPN)

Umfassende Sicherheit im gesamten Unternehmen

» Erhöhter Schutz durch Sicherheitssysteme im kompletten Netzwerk
» Transparenz & Kontrolle über diverse Zugriffe von innen & außen (egal von wo)
» Mitarbeiter*innen, Daten und Anwendungen auch aus der Ferne sichern können
» Vermeidung von Cyber-Angriffen & anderen Risiken bzw. frühzeitige Schadenseindämmung bei einem Vorfall
» nahtloser, transparenter End-to-End-Prozess

Compliance auf allen Ebenen

» Zero Trust als Prinzip für alle Bereiche Ihrer eingesetzten IT-Landschaft, um Security und Compliance umsetzen zu können
» durch den Zero-Trust-Ansatz wird bereits ein Großteil von Compliance-Richtlinien umgesetzt

07. Ihr Weg zu einer Zero-Trust-Architektur

Vorbereitung: Ist-Analyse und Strategie

Am Anfang steht die Bestandsaufnahme: Der erste Schritt sollte daher sein, dass Sie den Current Mode of Operation (CMO) Ihrer IT-Systemumgebung analysieren.

Folgende Fragestellungen können Ihnen dabei helfen

- » Gab es bereits Sicherheitsvorfälle und wenn ja, wo war die Schwachstelle?
- » Sind Ihre Identitäten durch Schutzmaßnahmen gehärtet?
- » Sind Ihre Endgeräte verwaltet (MDM) und besonders geschützt (AV/EDR/XDR)?
- » Schützen Sie Ihre vertraulichen Daten (DLP)?
- » Sind die Zugänge zu Ihren Netzen gesichert?
- » Werden Anwendungen und deren Daten verwaltet?
- » Setzen Sie eine feingranulare Infrastruktur mit Zugangsmanagement ein?

Je nachdem, wie Ihre Antworten ausfallen, haben Sie mehr oder weniger Handlungsbedarf. Davon abgeleitet erarbeiten Sie nun einen Future Mode of Operation (FMO) für Ihre sichere IT-Systemumgebung.

Umsetzung: Implementierung einer Zero-Trust-Architektur

Achten Sie bei der Umsetzung auf einen reibungslosen Übergang von Ihrer bestehenden zu der neuen bzw. erweiterten Infrastruktur. Neue Technologien bedeuten große Veränderungen. Denken Sie daher bereits zu Beginn des Projekts an ein professionelles Change Management, damit Ihre Kolleg*innen Ihre Entscheidungen mittragen und den Mehrwert erkennen.

Betrieb: Go-live und Evaluierung

Es ist Zeit, dass Ihr neues Sicherheitskonzept zum Einsatz kommt und gelebt wird.
Läuft alles, wie es soll? Gibt es Supportbedarf?

ORBIT ALS ZUVERLÄSSIGER PARTNER

Haben Sie Fragen und wünschen sich Beratung zur Umsetzung einer ganzheitlichen IT-Sicherheitsstrategie inklusive einer Zero-Trust-Architektur?

Dann nutzen Sie doch einfach unseren kostenfreien und unverbindlichen **Zero-Trust-Quickie** für einen ersten Austausch mit unserem Fachexperten **Benjamin Witt**.

In einem 30-minütigen Online-Gespräch haben Sie die Möglichkeit, drängende Fragen zu stellen und hilfreiche Tipps zu erhalten, wie Sie die IT-Sicherheit in Ihrem Unternehmen massiv erhöhen können.

ZERO-TRUST-QUICKIE BUCHEN

Benjamin Witt
Mobility Consultant

benjamin.witt@orbit.de

ORBIT Gesellschaft für Applikations- und Informationssysteme mbH
Mildred-Scheel-Str. 1 • 53175 Bonn • Tel. +49 228 95693-0
mailing@orbit.de • www.orbit.de

ORBIT IT-SOLUTIONS