DriveLock
securing your digital tomorrow

Vom Konzept zur Umsetzung:

In 6 Schritten zu mehr IT Sicherheit mit Zero Trust

eBook

DriveLock
securing your digital tomorrow

Warum beschäftigen sich IT-(Sicherheits-) Experten aktuell mit dem Konzept „Zero Trust“?

Einst haben Firewalls Unternehmen zuverlässig vor Bedrohungen geschützt. Für IT-Verantwortliche gab es eine klare Verteidigungslinie entlang der Grenzen von „Drinnen“ und „Draußen“. Neben immer intelligenteren Angriffen, Social Engineering oder Zero Day Exploits sorgen heute auch hybride Netzwerkgrenzen für eine höchst komplexe IT-Sicherheitslage.

Der Zero Trust Ansatz hilft CIOs und Sicherheitsverantwortlichen, sich diesen Herausforderungen zu stellen. Im Fokus des Konzepts steht der Schutz sensibler und kritischer Daten. Zero Trust berücksichtigt dabei die heutigen heterogenen Infrastrukturen mit einer Vielzahl zu schützenden Geräten und behandelt dabei jeden Zugriff, jede Anwendung, jedes Gerät mit der gleichen Vorsicht – egal ob intern oder extern. **Mit anderen Worten: Zero Trust – der Name verrät es – vertraut niemanden und setzt auf stetige Überprüfung.**

Was heißt das nun konkret? Mit den folgenden sechs Schritten zeigen wir Ihnen, wie Sie Zero Trust in der eigenen Organisation umsetzen und damit einen umfassenden Schutz unternehmenskritischer Daten gewährleisten.

DriveLock
securing your digital tomorrow

Schritt 1

Legen Sie in einem Assessment den organisatorischen Rahmen fest.

Stellen Sie sich folgende Fragen:

- Was wollen Sie weshalb schützen?
- Befinden sich die digitalen und physikalischen Assets auf eigenen Servern oder in der Cloud?
- Welche Daten haben Sie als öffentlich klassifiziert und welche Daten sind dagegen hochsensibel?
- Erlaubt Ihr Unternehmen, auch eigene Endgeräte zu nutzen? (BYOD)
- Nutzen Sie externe Datenträger (z. B. USB-Sticks)?
- Welche Touchpoints mit Mitarbeitern, Partnern, Zulieferern oder Endkunden gibt es?
- Wie, von wo und über welches Medium erfolgt der Zugriff auf Ihr Unternehmensnetzwerk?

Bedenken Sie:
Ihr Unternehmensnetzwerk besteht nicht nur aus Desktops und Laptops! U. a. erweitern mobile Endgeräte wie Handys, Virtual Environments und virtuelle Desktop-Infrastrukturen die Netzwerkgrenzen.

TIPP 1:

Firmenrichtlinien für Sicherheit und Geräte spielen eine bedeutende Rolle

Erlaubt Ihr Unternehmen „Bring Your Own Device", sind die Sicherheitsrisiken potentiell höher. Dürfen nur firmeneigene Geräte verwendet werden, sind die Mitarbeiter dagegen stärker eingeschränkt.

TIPP 2:

Einschränkungen können auch für Wechseldatenträger gelten

Sie können auf USB-Sticks Schreibrechte verweigern oder die Nutzung sogar gänzlich verwehren. Bestimmte Anwender, z. B. Wartungsmitarbeiter für Produktionsanlagen können dagegen auch erweiterte Rechte erhalten, um eigene USB-Sticks anzuschließen und Daten auszutauschen.

Grundsätzlich wichtig:

Der Sicherheitsverantwortliche in Ihrem Unternehmen sollte wissen, wie die Prozesse innerhalb Ihres Unternehmens aussehen und welche Geräte, Applikationen, Dienste und Workloads wie verwendet werden.

Für eine erfolgreiche Einführung von Zero Trust ist es unbedingt entscheidend, alle betroffenen Personen im Unternehmen einzubeziehen.

DriveLock
securing your digital tomorrow

Schritt 2

Machen Sie eine Inventur der Hardware und Software.

Im nächsten Schritt visualisieren Sie alle Daten in einer Bestandsaufnahme, um weitere sicherheitsrelevante Aspekte und potentielle Schwachstellen zu ermitteln. Ihre Inventur sollte die gesamte angeschlossene Hardware, die Software und Betriebssysteme umfassen.

Fragen aus der Bestandsaufnahme sind z. B.:

- Haben Sie alle Updates und Patches aufgespielt?
- Gibt es noch Support vom Hersteller oder ist das System bereits veraltet?

Wichtig: Welche Bedeutung diese Punkte für Ihre IT-Sicherheit haben, verdeutlich die verheerenden Folgen des Trojaners WannaCry, die dazu führten, dass Microsoft sich entschied, auch für das veraltete Windows XP noch einen Patch zu liefern.

Mit einer Lösung für automatisiertes Schwachstellen- und Patch-Management erleichtern Sie diese Arbeit erheblich.
Ein Überblick über das Security Posture, also den Zustand und die aktuellen Einstellungen aller Endpunkte, leitet den nächsten Schritt drei ein.

DriveLock
securing your digital tomorrow

Schritt 3

Prävention: Diese Werkzeuge sollten Sie kennen.

Es gibt zahlreiche Maßnahmen, um Cybergefahren von vornherein zu eliminieren und Datenintegrität zu gewährleisten. Institutionen wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder das Center of Information Security stellen umfassende Leitfäden zur Verfügung.
Die folgenden Werkzeuge sollten aus unserer Sicht im Rahmen Ihrer Präventionsmaßnahmen eine Rolle spielen.

TIPP 1:

Festplatten-, File & Folderverschlüsselung

Verschlüsseln Sie stets Festplatten und Dateien, egal ob auf mobilen Datenträgern, lokalen Servern oder in der Cloud. Richtlinien für Datenverschlüsselung auf Wechseldatenträgern helfen Ihnen, sich vor Verlust, Diebstahl und Industriespionage zu schützen.

TIPP 2:

Nutzen Sie Device Control

Datenträger- und Datenflusskontrolle ist enorm wichtig, denn USB-Sticks sind nach wie vor ein Einfallstor für Schadsoftware und Datenklau. Richtlinien müssen klären, wer was mit welchen Geräten und Datenträgern machen darf.

TIPP 3:

Application Control mit Whitelisting

Erlauben Sie ausschließlich die Ausführung vertrauter und erlaubter Anwendungen, die auf der „Whitelist" stehen.
Das gewährleistet bestmöglichen Schutz vor Zero-Day Exploits, also noch unbekannten oder nicht-gepatchten Sicherheitslücken sowie neuer Malware.

Ergänzende Info:
www.av-test.org registriert z. B. pro Tag 350.000 neue Malware-Programme. Ein Sicherheitsnetz, das Firewalls und Antivirenprogramme ergänzt, ist daher essentiell. Dank Application Control wird Schadsoftware, die es dennoch ins System schafft, nicht ausgeführt. Zudem sollten Sie keine lokalen Administrationsrechte vergeben, damit Anwendungen nicht ungeprüft heruntergeladen und installiert werden können.

TIPP 4:

Identity & Access Management

Zugriffskontrolle ist eine weitere kritische Sicherheitsmaßnahme, insbesondere dort, wo schwache Passwörter vergeben werden. Mit Hilfe von 2-Faktor- oder Multi-Faktor-Authentifizierung schützen Sie sich so beispielsweise vor den Folgen von Social Engineering. Angreifer erhalten trotz erbeuteter Login-Daten keinen Zugriff auf Ihre Daten und Systeme.

Schritt 4

Detection & Response – Erkenntnis ist der erste Schritt zu mehr IT-Sicherheit.

TIPP 1:

Detection Tools

Sogenannte Detection Tools erkennen bestimmte Aktionen, Muster oder Applikationen und setzen sie in einen Zusammenhang. So ermitteln sie Anomalien und potentiell gefährliche Verhaltensmuster. Wenn z. B. unverhältnismäßig viele Dateien auf einen Wechseldatenträger kopiert werden, könnte das auf Industriespionage hindeuten.

TIPP 2:

File Reputation Services

Diese helfen Ihnen bei unbekannten Anwendungen, die richtige Response-Maßnahme zu treffen und eine Applikation z. B. zu blacklisten. Diese Listen sammeln alle Informationen zu Applikationen und stellen sie öffentlich zur Verfügung, denn nicht alles Unbekannte muss zwangsläufig auch gefährlich sein. Bei Bedarf können Geräte abgeschaltet, vom Netz genommen oder unter Quarantäne gestellt und Prozesse abgebrochen werden.

TIPP 3:

Analyse- und Forensik

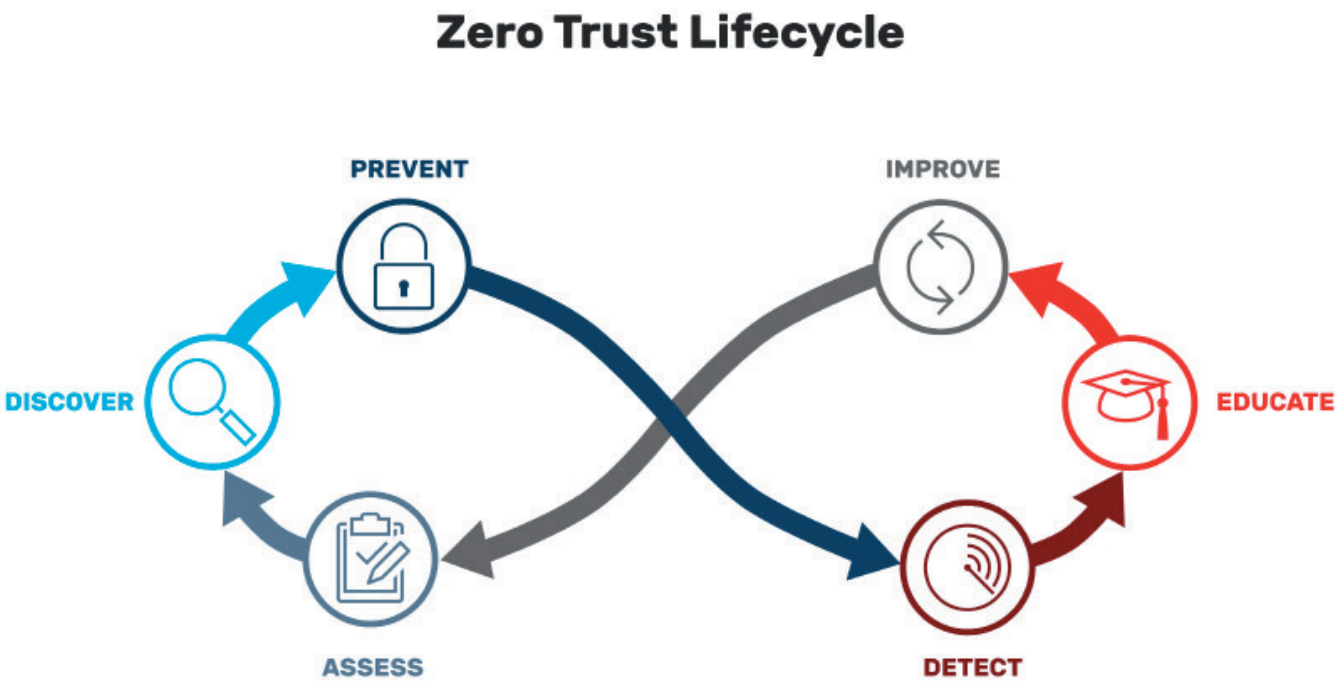
Analyse- und Forensik-Funktionen ermöglichen Ihnen festzustellen, wie Malware in das System gelangt ist. Mithilfe dieses Wissens können weitere Response-Maßnahmen abgeleitet werden.

Speisen Sie die Daten zusätzlich in eine Security-Incident- und Event-Management-Lösung wie Splunk oder Logrhythm ein, profitieren Sie von zusätzlichen Funktionen wie Alerting und automatisierter Priorisierung.

Schritt 5

Kontinuierliche Verbesserung – Nach dem Prozess ist vor dem Prozess.

Wie bei vielen Dingen im digitalen Leben ändert sich auch die IT-Bedrohungslage rasant und eine Evaluation der Risiken sollten Sie immer wieder und insbesondere nach einschneidenden Ereignissen durchführen.
Anlass kann z. B. eine Umstrukturierung im Unternehmen sein, die Einführung einer unternehmensweiten Software (z. B. SAP) oder andere größere Software- und Website-Projekte.



Wichtig: Sie sollten den gesamten Zero Trust Prozess in regelmäßigen Abständen immer wieder neu beginnen, um das Sicherheitslevel in der Organisation stets auf dem höchsten Stand zu halten.

DriveLock
securing your digital tomorrow

Schritt 6

Nehmen Sie Ihre Mitarbeiter mit.

Sensibilisierung durch Security Education

Alle Sicherheitsmaßnahmen der vorangegangenen Schritte greifen erst dann optimal, wenn die gesamte Belegschaft an einem Strang zieht.

Natürlich sind Sicherheitsmaßnahmen auch mit Einschränkungen verbunden, die Mitarbeiter frustrieren. In digitalen Zeiten sind wir es gewohnt, selbstbestimmt zu arbeiten und wollen uns nicht gern einengen lassen. Machen Sie immer wieder deutlich, dass ALLE Mitarbeiter ein wichtiger Teil der gesamten Sicherheitsstrategie sind.

Regelmäßige und anlassbezogene, z. B. wenn ein Mitarbeiter einen externen USB-Stick anschließt, Schulungen und Kommunikationsmaßnahmen schaffen das nötige Sicherheitsbewusstsein und verhindern Frustration.

DriveLock
securing your digital tomorrow

FAZIT | Zusammen gestalten.

Zero Trust ist ein Zusammenspiel von mehreren, sich ergänzenden Sicherheitsmaßnahmen mit dem strategischen Ziel, Datenintegrität zu gewährleisten und Datenschutzverletzungen zu verhindern.

Das Zero Trust Konzept erreicht dieses Höchstmaß an IT-Sicherheit, indem es so viele **Hürden und Einschränkungen** wie möglich errichtet und **alle Assets, Anwender und Aktionen im System** überprüft.
In Zeiten der digitalen Transformation hängt der Erfolg von Unternehmen maßgeblich davon ab, wie zuverlässig Menschen, Unternehmen und Dienste vor Cyber-Angriffen und vor dem Verlust wertvoller Daten geschützt sind.

Wir haben uns zum Ziel gesetzt, Unternehmensdaten, -geräte und -systeme zu schützen.
Unsere Zero-Trust-Plattform vereint die Elemente.

- **Data Protection**
- **Endpoint Protection**
- **Endpoint Detection & Response**
- **Identity & Access Management**

Unsere voll integrierte Zero-Trust-Plattform unterstützt unterschiedliche Betriebssysteme, Endgeräte und wird als On-Premise-Lösung und Managed Security Service angeboten. Die Lösung ist Made in Germany und „ohne Backdoor".

Kontaktieren Sie uns!

DriveLock SE
+49 (89) 546 36 49-0
info@drivelock.com

www.drivelock.com