Herbsttagung 2020
Zero Trust: Weg vom Perimeter… hin zu …

Urs Wagner
cnlab

Rolf Wagner
FORTIT
SECURE DIGITAL BUSINESS

Zürich, 9. September 2020

Agenda_

- Die alte Welt: Perimeterschutz
- Die neue Welt: Zero Trust
- Technologien und Ausblick

Die alte Welt

Firmennetze:

- Perimeterschutz auf Netzwerkebene
- Einkommend: Firewall / NAT
- Ausgehend: Proxy
- Innerhalb: implizites Vertrauen

Die alte Welt und die Sicherheit

1. Opfer aussuchen (LinkedIn)
2. Opfer infizieren (Waterholing)
3. Infektion innerhalb des Netzes ausbreiten

Citrix: Angreifer dringen ins Firmennetz ein

Das US-Unternehmen Citrix meldet einen Einbruch in sein Intranet. Cyberkriminelle hätten Geschäftsdokumente erbeutet – viel mehr ist noch nicht bekannt.

APT Case RUAG

Technical Report

extensive *fingerprinting* before and after the initial infection. After they got into the network, they moved laterally by infecting other devices and by gaining higher privileges. One of their main targets was the *active*

Konzeptionelle Schwierigkeit:
- Bedürfnis: Vernetzung
- Schutz: auf Netzwerkebene

Eigentliches Ziel:
- Schutz der Daten

Die alte Welt und die Bedürfnisse

Sowohl die Endgeräte wie auch die Dienste sind mobil

- Cloud
- SaaS
- Homeoffice
- BYOD

Frage:

- Wo ist der Firmennetzwerkverkehr?
- Wo ist der (Netzwerk-)Perimeter?

Alte Welt adieu…

Sicherheit:

- Perimeter ist nicht dicht
- «falsche Sicherheit»
- APT

→ Man sollte sich nicht auf Netzwerkperimeter verlassen

Neue Bedürfnisse:

- Arbeiten von überall
- Mit verschiedensten Geräten
- Verschiedenste (Cloud-) Dienste
- Software as a Service

→ Klar abgrenzbares Firmennetz nicht realisierbar

Ziel:

- Schutz der Daten / Ressourcen in einem veränderten Umfeld
- Idealerweise: Einheitliche Benutzererfahrung

Zero Trust

✓ **Kontextsensitiver, adaptiver Schutz der Ressourcen**
(Services, Workloads, Applikationen, Daten)

✓ **Least Privilege**

✓ **Assume Breach**

✓ **Never Trust, Always Verify**

✗ **Statische Verteidigung von traditionellen Netzwerk Perimetern**

✗ Trust in Netzwerke

✗ Trust in Interfaces

✗ Trust in Users

Zero Trust – «Wer hat's erfunden?»

AuthN: Authentication
AuthZ: Authorization

2010

Zero Trust –
Never Trust, Always Verify

"The Zero Trust Network Architecture" von John Kindervag (Forrester)

- Konsequente Zugriffskontrolle
- Keine "sicheren" Netzwerkzonen
- Traffic Monitoring

Einige (erweiterte) Zero Trust Auslegungen

Forrester ZTX - Zero Trust eXtended
Erweiterungen insbesondere hinsichtlich Überwachung und Automatisierung

Gartner CARTA - Continuous Adaptive Risk and Trust Assessment
Adaptive, kontextsensitive Sicherheitssysteme; Kontinuierliche Risiko- und Vertrauensbewertung

Google BeyondCorp
Remove trust from network; Zugriffssteuerung nutzt alle verfügbaren User & Device-Informationen; Kein Zugriff ohne AuthN, AuthZ und Encryption

Microsoft Zero Trust
Nutze alle Informationspunkte für AuthN, AuthZ; Least Privilege Prinzip; Assume Breach – Minimierung der Schadensschneise

Zero Trust Building Blocks – Vorher / Nachher

AuthN: Authentication
AuthZ: Authorization

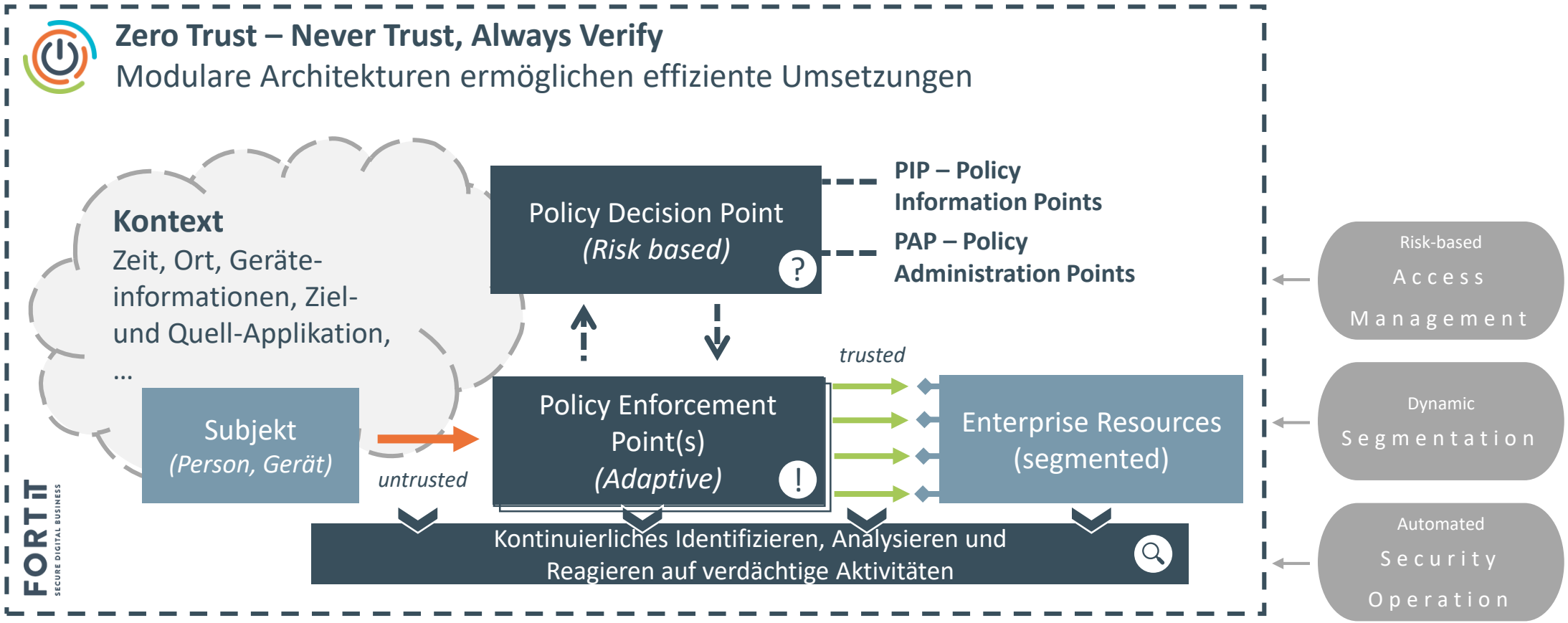
Zero Trust – Never Trust, Always Verify

Drei grundsätzliche Handlungsfelder für die iterative Umsetzung von ZT

	Traditional	Zero Trust
Access Management	• Pauschal-Authorisierung aufgrund Netzwerk • Statische AuthN-Level	• Risiko-basierte, adaptive und feingranulare AuthN und AuthZ (User & Device)
Segmentation	• Statisch, HW-Config • Perimeter-basierend (Inside = Trusted, Outside = Untrusted)	• Dynamisch, feingranular, Software-Defined • Policy-basierend je Service Applikation, Workload
Security Operation	• Fokus auf die Analyse und Kontrolle bei Perimeter-übergängen • Reaktiv bei Incidents	• Kontinuierliche Analyse von (User) Aktivitäten • Proaktive Nutzung für (Re-) AuthN & AuthZ

FORTIT SECURE DIGITAL BUSINESS

Zero Trust Building Blocks – Mapping auf die Zugriffskontrolle



FORTIT SECURE DIGITAL BUSINESS

Legokasten

Zugriffskontrolle

- Starke Authentisierung
  - Fido2, mTLS
- Adaptive Authentisierung
  - Conditional Access
- Benutzerfreundlich: SSO
- Endgeräte
  - Device Policies, TPM, Secure Enclave

Vortrag: Zuzana Trubini

Demos:

- René Vogt
- Thomas Lüthi

Segmentierung

- Containerlösungen
  - Kubernetes / Openshift
  - Istio
- SDN

Vortrag: Stephan Verbücheln

Demo: Stefan Kunz

Security Operations

- SIEM
- Device Management

Vortrag: Thomas Fröhlich

«Das haben wir doch schon alles»

Die Kunst ist:

- Gute Architektur
- PDP
  - Zentralisierung
  - Entscheidungslogik
- Nachvollziehbare
  - Zugriffsentscheide
  - Authentisierungsaufforderungen
- Geräteintegrität / Schwachstellenmanagement

PEP & PDP

- Früher: Anwendung, PEP und PDP in Personalunion
- Heute:
  - PDP zentral
  - PEP nahe bei Ressource
- Zugriffsbeschränkung:
  - Netzwerkebene (Firewall)
  - Vertraue Cloudanbieter
  - mTLS
  - Kubernetes / Openshift Mechanismen

Vielen Dank für Ihre Aufmerksamkeit_

urs.wagner@cnlab.ch
+41 55 214 33 42

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

rolf.wagner@fort-it.ch
+41 58 255 09 57

FortIT AG
Waldmannstrasse 10
8001 Zürich-Bellevue
+41 58 255 09 55
www.fort-it.ch