genua Ein Unternehmen der Bundesdruckerei

Security Defined Networking:

a Necessity for Critical Infrastructures

Arnold Krille

Omnisecure – 21.01.2020

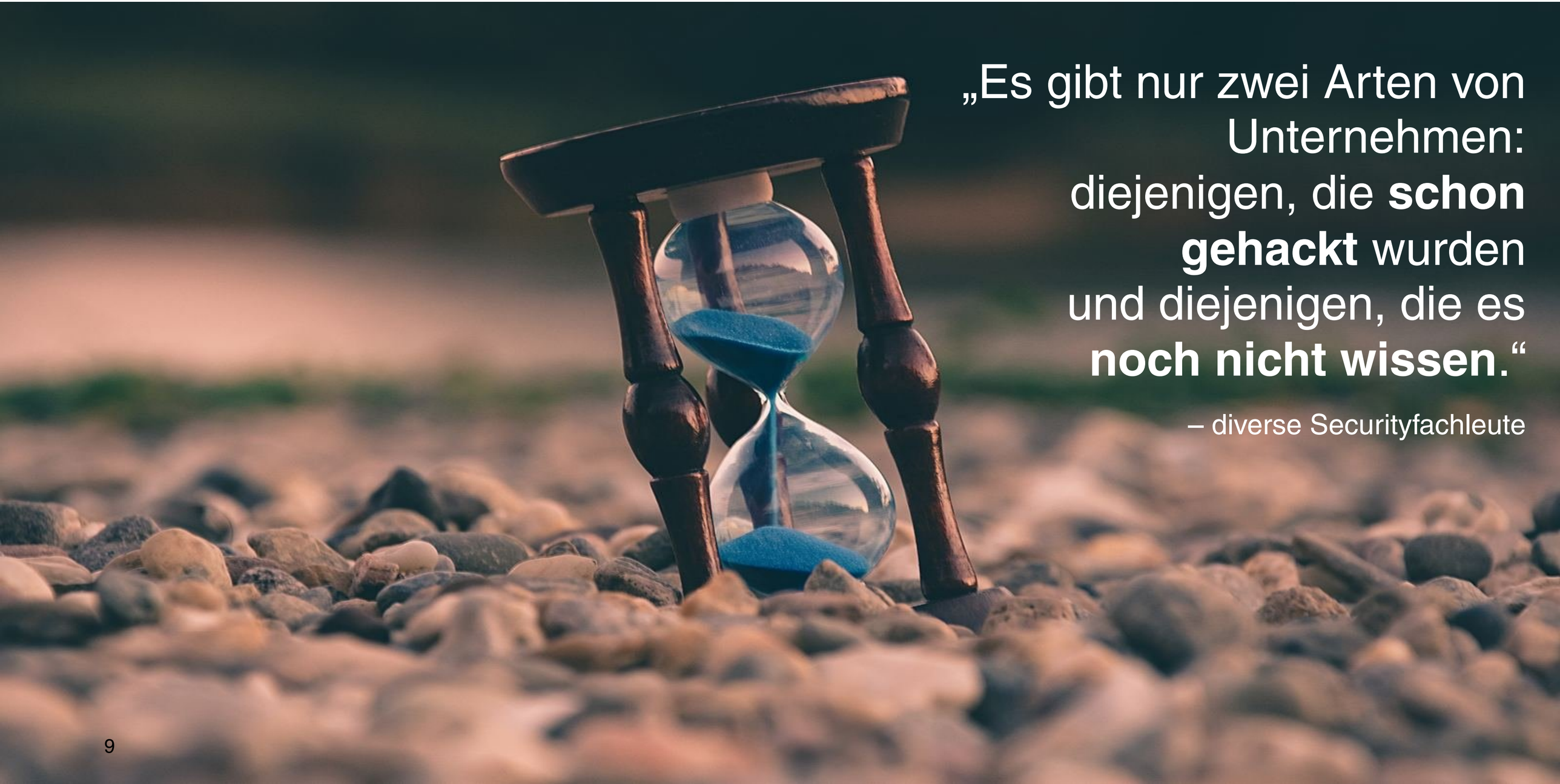
- Arnold Krille
  - MLU Halle-Wittenberg — Forscher / Entwickler / Admin
  - bcs kommunikationslösungen — Administrator / Entwickler
  - gateprotect Leipzig GmbH — Software Entwickler
  - gateprotect GmbH
  - Rohde & Schwarz Cybersecurity GmbH
  - Packetwerk GmbH — Entwickler / Produktmanager
  - cognitix GmbH — COO / CEO
  - genua GmbH — Abteilungsleiter

- genua GmbH:
  - junges Startup von 27 Jahren
  - Experte in Netzwerksicherheit
  - Ein Unternehmen der Bundesdruckerei
    ein junges Startup von >180 Jahren ;-)
- cognitix:
  - Startup von <2 Jahren
  - Nun ein Teil der genua GmbH

State-of-the-Art

- Netzwerk von Außen schützen: Firewall am Perimeter
- Geschützter Zugang von Außen in das Netzwerk: VPN
- Netzwerksegmentierung mit gesicherten Übergängen: Firewall, Daten-Dioden, Fernwartungsrendevousserver
- Sicherheit der Clients und Server selber: Endpoint Security, Antivirus, Application-Gateways und Proxies
- Übergreifende Überwachung durch zentrale Auswertung von Log-Files und durch Monitoring von Diensten


There are only two types of Companies:
Those that **have been hacked**,
and those **that will be**.
Robert Mueller, FBI Director, 2012

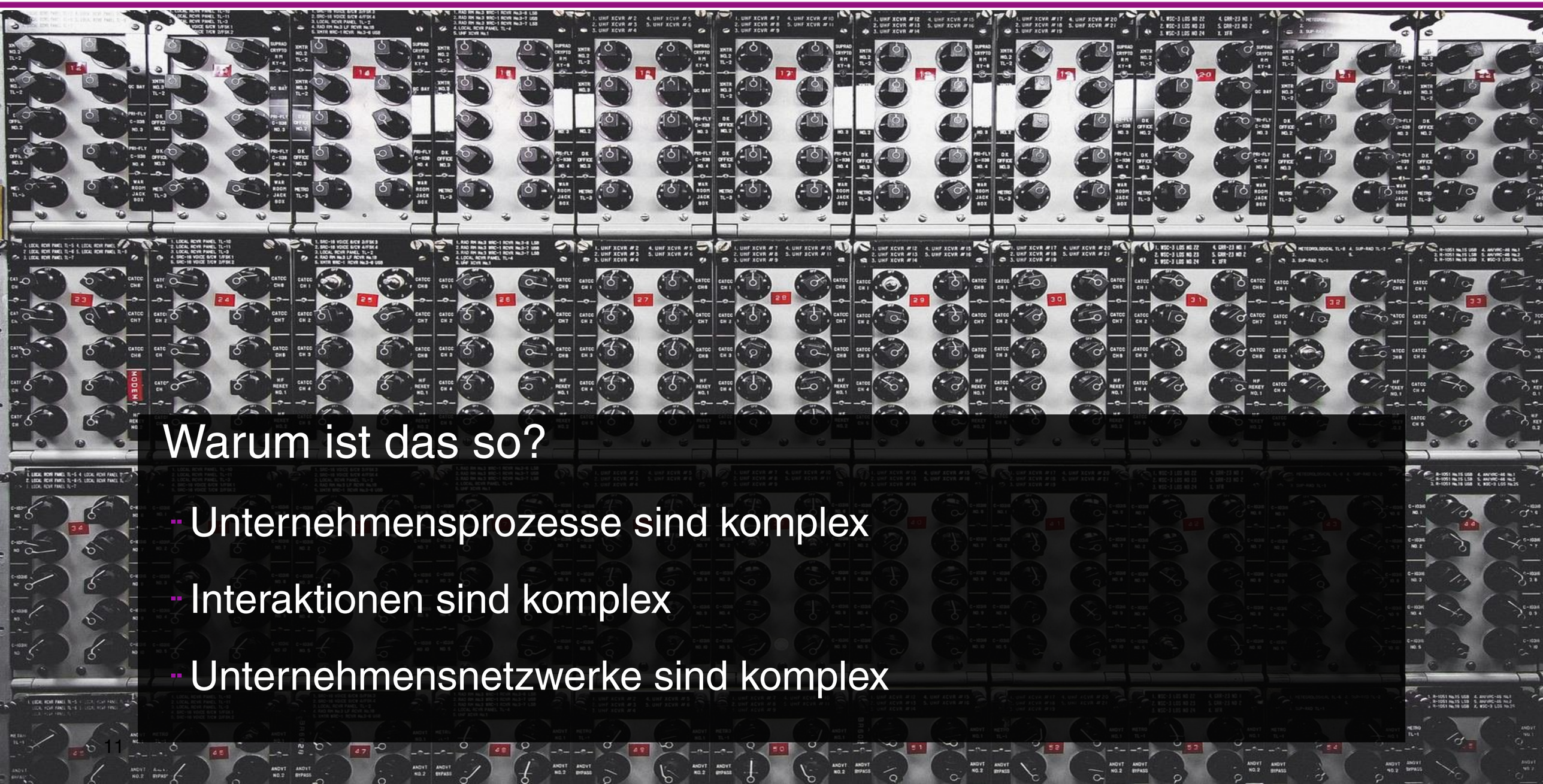


„Es gibt nur zwei Arten von Unternehmen: diejenigen, die **schon gehackt** wurden und diejenigen, die es **noch nicht wissen**.“

– diverse Securityfachleute

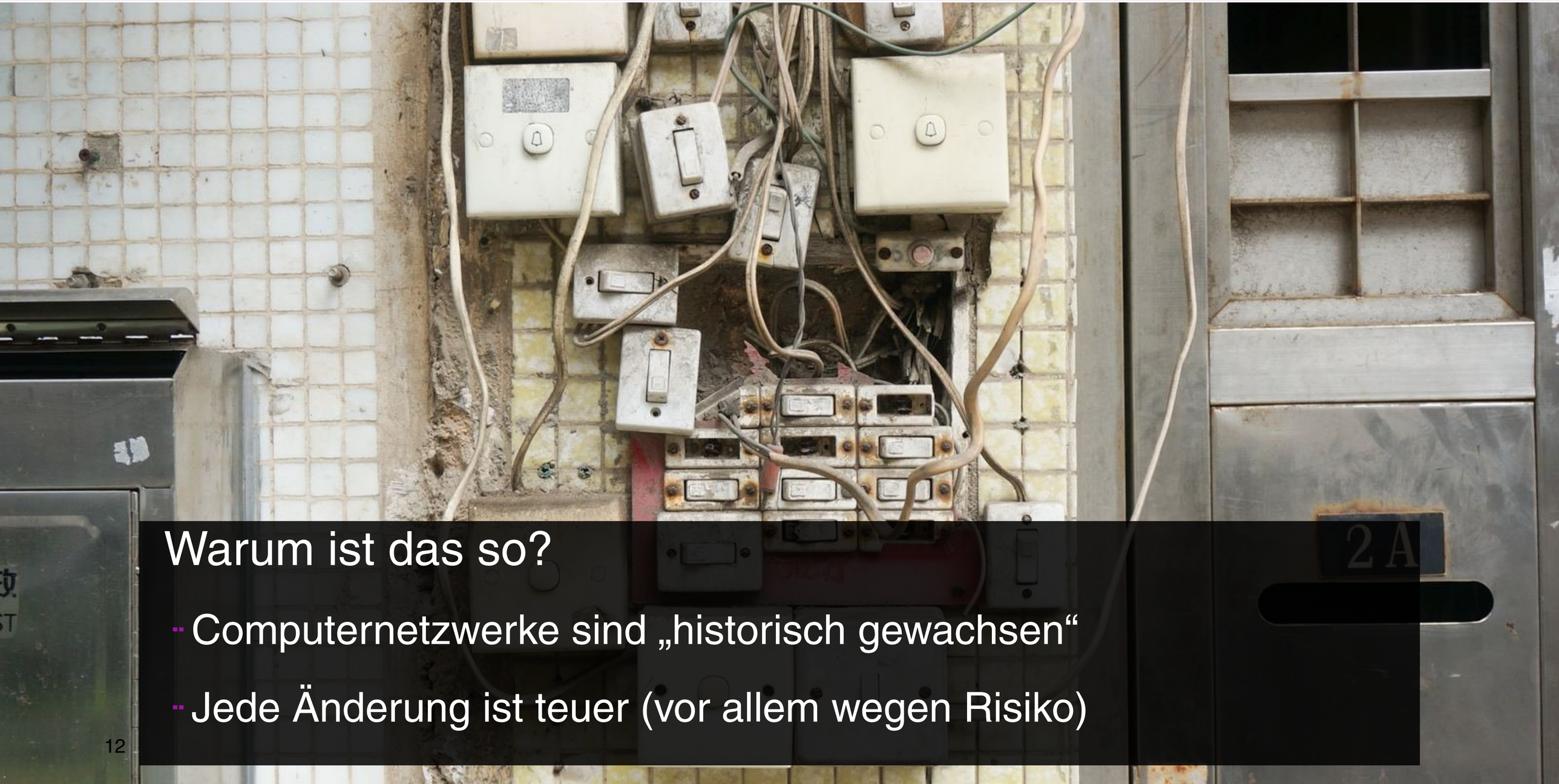
80% Angriffe mit Innentäter

genua Ein Unternehmen der Bundesdruckerei



Warum ist das so?

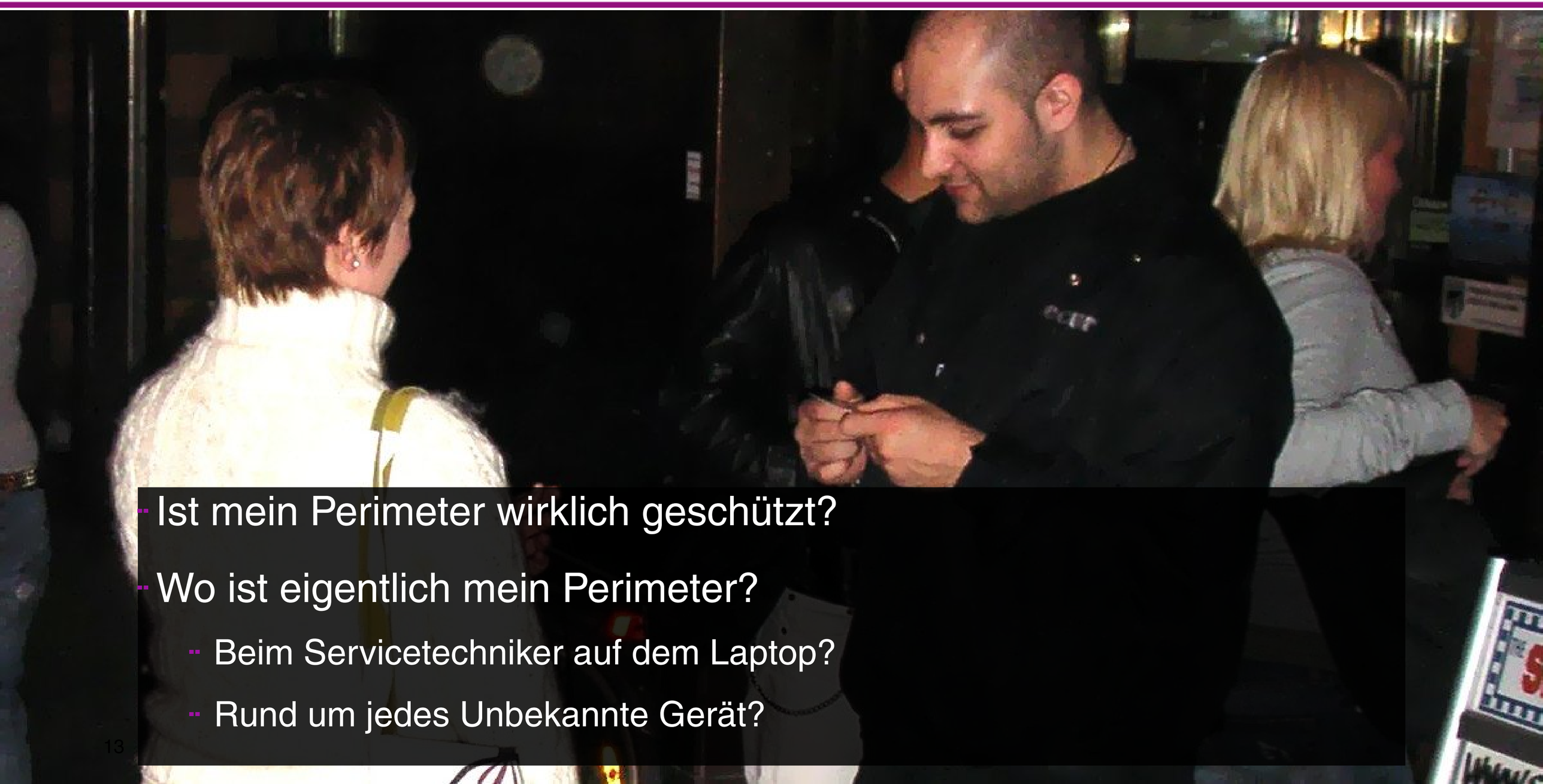
- Unternehmensprozesse sind komplex
- Interaktionen sind komplex
- Unternehmensnetzwerke sind komplex



Warum ist das so?

- Computernetzwerke sind „historisch gewachsen“
- Jede Änderung ist teuer (vor allem wegen Risiko)

Schutz nur am Perimeter?



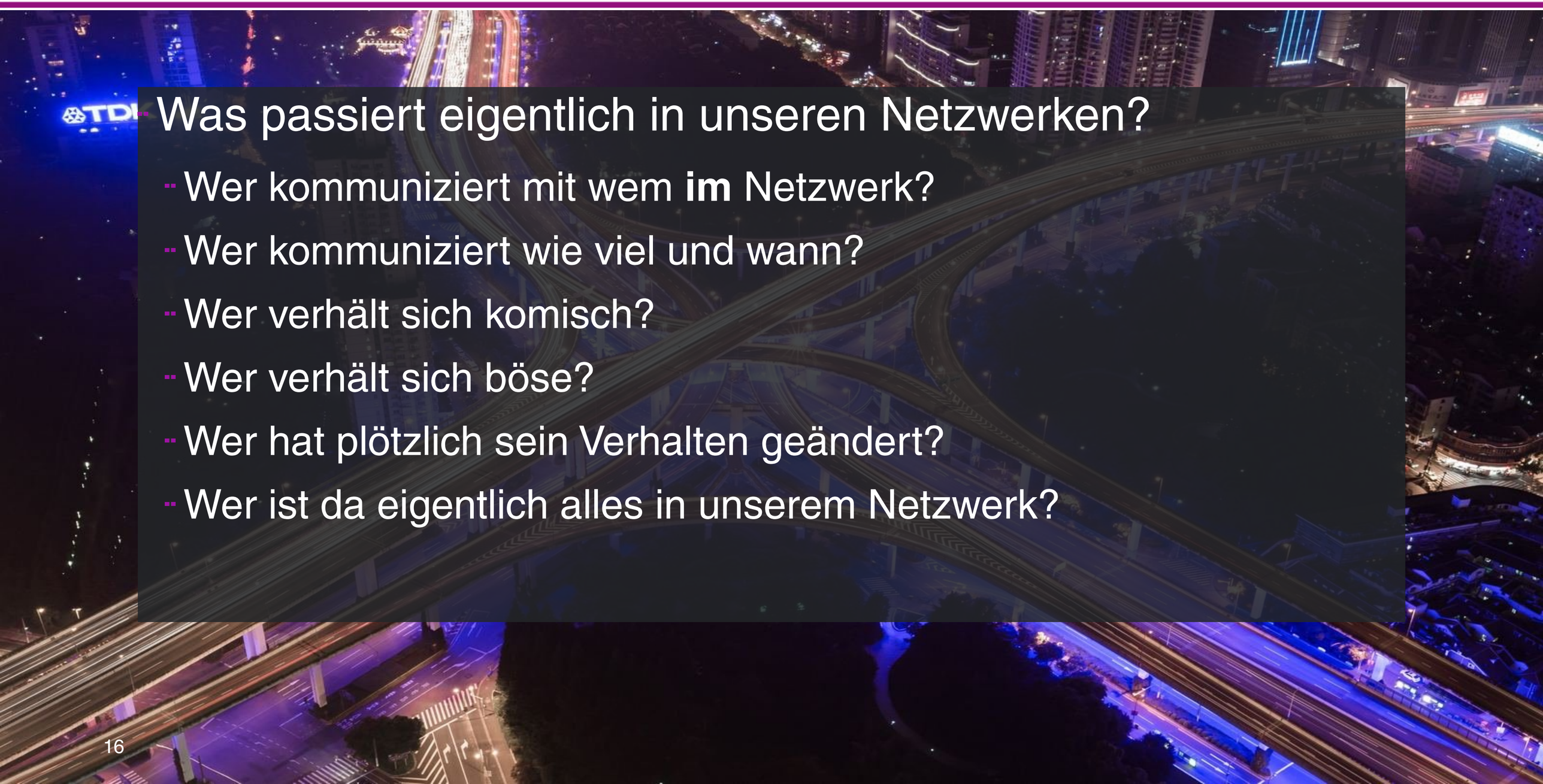
- Ist mein Perimeter wirklich geschützt?
- Wo ist eigentlich mein Perimeter?
  - Beim Servicetechniker auf dem Laptop?
  - Rund um jedes Unbekannte Gerät?

Wer ist eigentlich in meinem Netzwerk

Viel mehr Geräte als nur PCs und Server:
Handys, Tablets, VoIP, Fernseher, Überwachungskameras, Anlagensteuerungen, Smart Things (IoT, iIoT, Industrie 4.0), und ganz neu™: Netzwerkdrucker

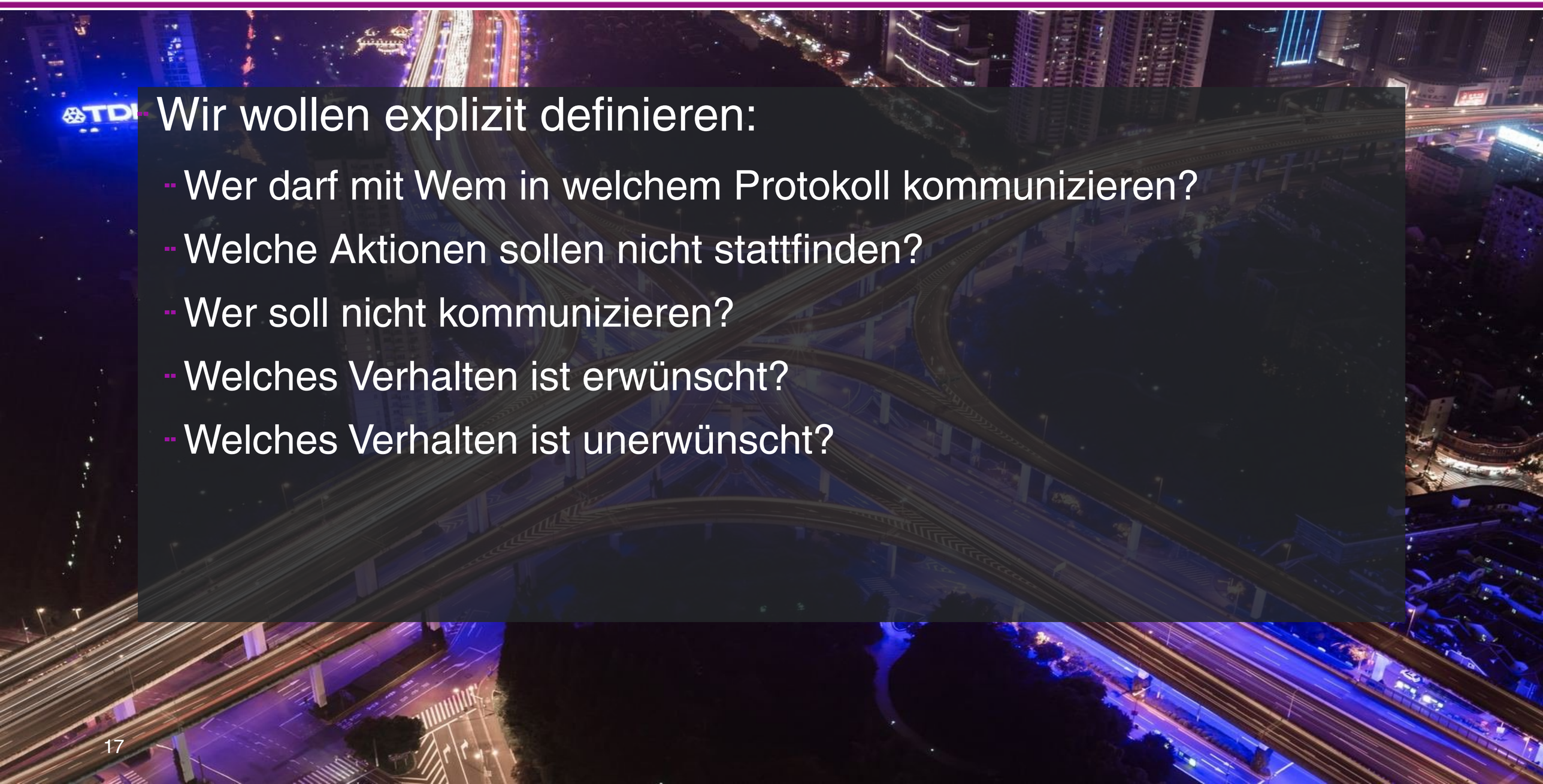
Was nun?

Was wollen wir?



- Was passiert eigentlich in unseren Netzwerken?
  - Wer kommuniziert mit wem **im** Netzwerk?
  - Wer kommuniziert wie viel und wann?
  - Wer verhält sich komisch?
  - Wer verhält sich böse?
  - Wer hat plötzlich sein Verhalten geändert?
  - Wer ist da eigentlich alles in unserem Netzwerk?

Was wollen wir?



- Wir wollen explizit definieren:
  - Wer darf mit Wem in welchem Protokoll kommunizieren?
  - Welche Aktionen sollen nicht stattfinden?
  - Wer soll nicht kommunizieren?
  - Welches Verhalten ist erwünscht?
  - Welches Verhalten ist unerwünscht?

Stichwort

Security Defined Networking

genua Ein Unternehmen der Bundesdruckerei

Security Defined Networking:

- Volle Sichtbarkeit aller Geräte und allen Netzwerkverkehrs
- Volle Erfassung und Modellierung des Verhaltens der Geräte
- Volle Kontrolle über Netzwerkverkehr und -verhalten

genua Ein Unternehmen der Bundesdruckerei

Security Defined Networking:

- Das Verhalten des Gerätes/Nutzers bestimmt die effektiven Sicherheitsbestimmungen im Netzwerk.
- Flexibler Schutz des Netzwerkes basierend auf Verhalten (Game Changer!)

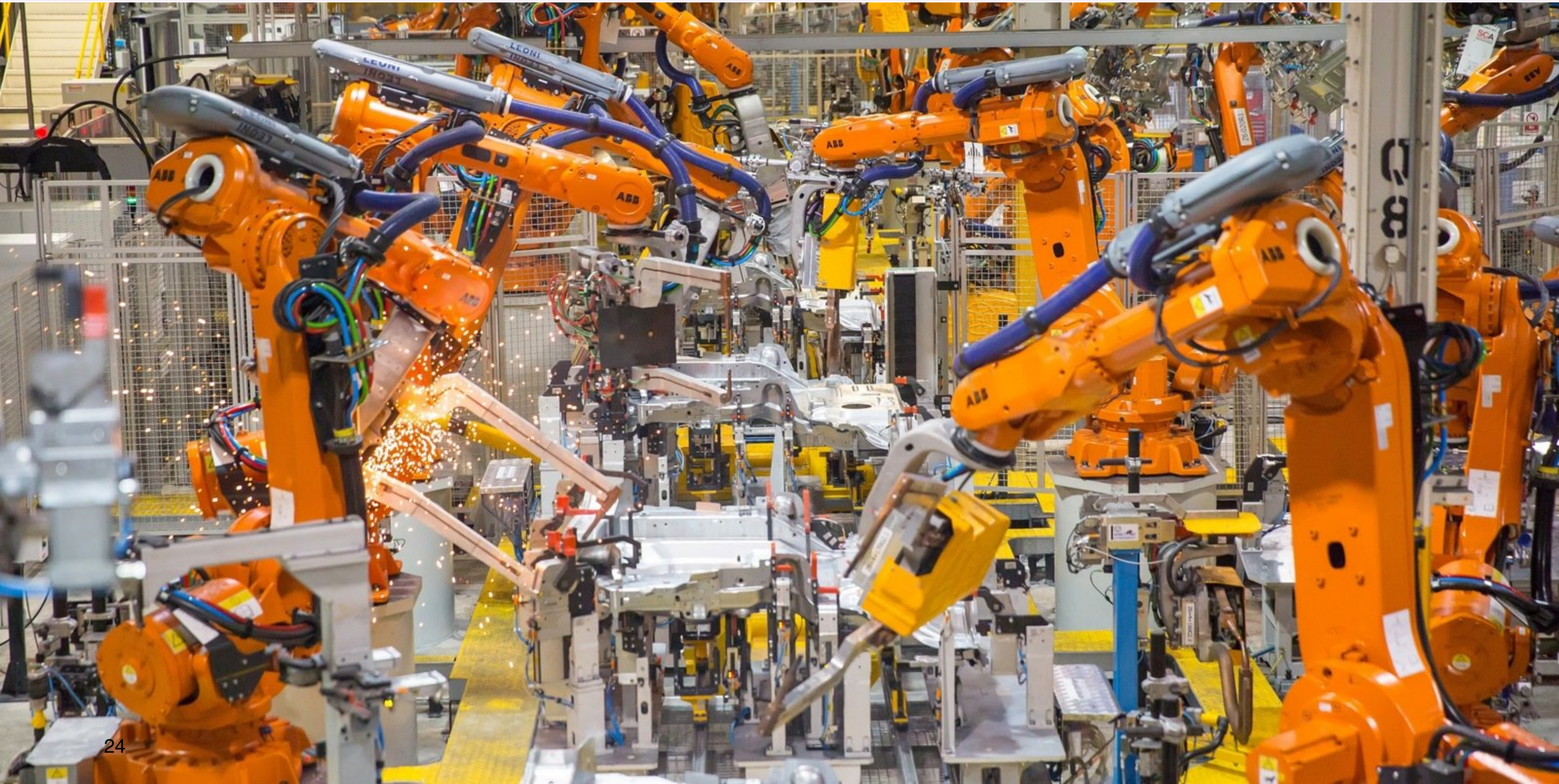
Security Defined Networking

- Security losgelöst von Infrastruktur
- Flache Infrastruktur möglich, dennoch Security
- Security / Segmentierung in flachen Netzwerken als Drop-In in Legacy Netzwerken
- Für Sicherheit im Netzwerksegment
  - und auch am Perimeter im Zusammenspiel mit Firewall und VPN.
- einfache Infrastruktur, einfaches Management

Harte Schale + harter Kern

Anwendung in Unternehmensnetzwerken

Anwendung in der Industrie



Drop-In Security in existierenden Netzwerken

genua Ein Unternehmen der Bundesdruckerei

Vielen Dank für Ihre Aufmerksamkeit!

Vielen Dank für Ihre Aufmerksamkeit!

Mehr Informationen zur **Technologie**, der Person, der Firma und den **Produkten** bei mir.

Und am **Stand der genua GmbH**.

Anhang für Fragen

„Da gibt‘s doch was von genua?“

genua Ein Unternehmen der Bundesdruckerei

FÜR IHR UNTERNEHMEN

IT-Sicherheitslösungen ist Ihr Unternehmen vor Cyber-Angriffen umfassend geschützt – auch im Geheimschutzbereich.

FILIALE

genuscreen: Netzwerk- und Datensicherheit

PRODUKTIONSSTANDORT

cyber-diode: Monitoring kritischer Systeme

genubox: Sicher kontrollierte Fernwartung

GS.Gate: Risikofreie Datenanalyse und Produktionsoptimierung

genuwall: Für Sicherheitszonen im Produktionsnetz

ZENTRALE

genugate: Robuster Netzwerkschutz im Unternehmen

genucenter: Komfortable und effiziente Administration

genua Advanced Secure Connect: Fernwartung sensibler SAP-Systeme

MOBILE MITARBEITER

cyber-top: Unterwegs geschützt dank Mobile Security

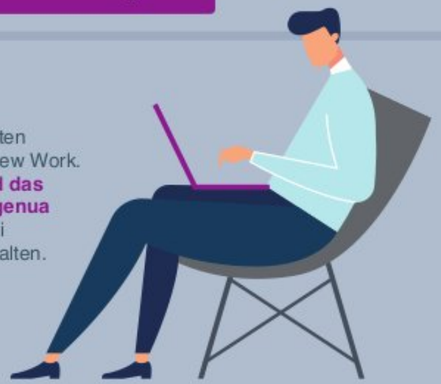
HOMEOFFICE

genucard: IT-Sicherheit im Homeoffice

Mit der **genuscreen** tauschen wir sensible Daten zwischen unseren Standorten aus – natürlich hochsicher verschlüsselt.

Die **Industrial Security-Lösungen** von genua schützen unsere Produktionsnetze, Anlagen und Daten umfassend vor Cyber-Angriffen.

Wir profitieren von digitalisierten Wertschöpfungsketten und New Work. **IT-Sicherheitslösungen und das zentrale Management von genua** gewährleisten, dass wir dabei unsere Security Policies einhalten.

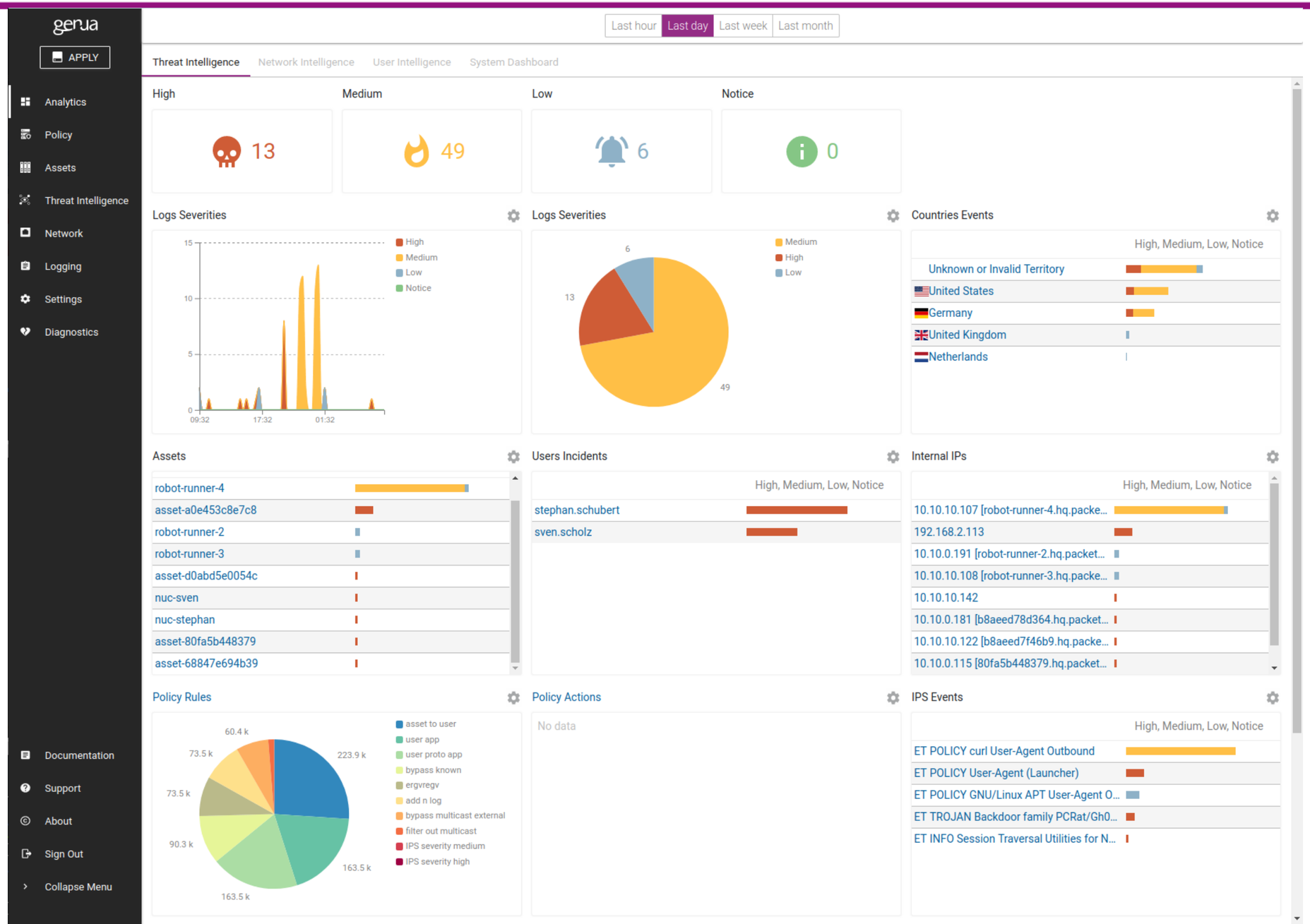


Unsere **Security Laptops** schützen vertrauliche Firmendaten auch unterwegs und erlauben so mobiles Arbeiten.

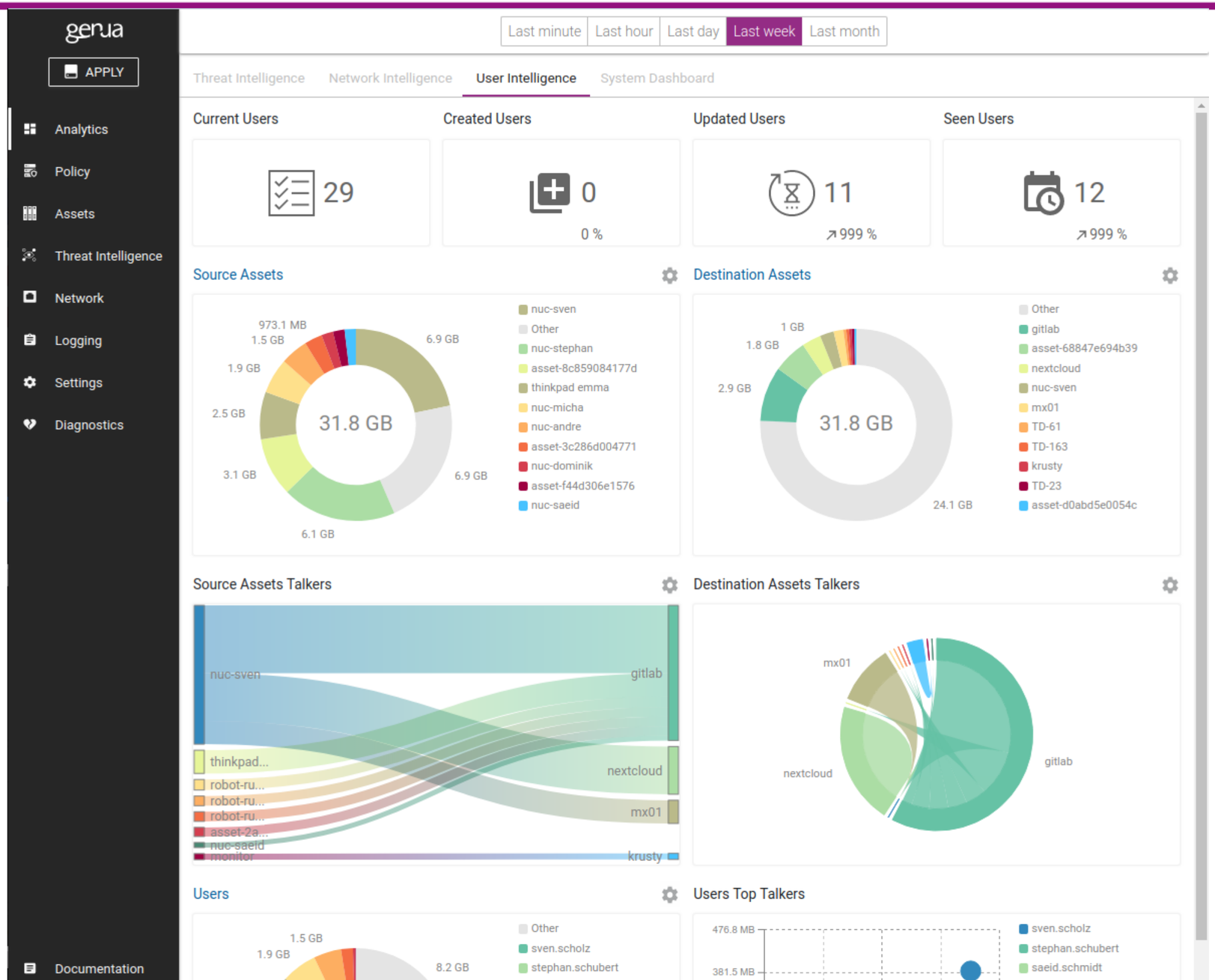
Dank der **genucard** arbeiten unsere Mitarbeiter flexibel und sicher im Homeoffice.

Teaser: cognitix Threat Defender

genua Ein Unternehmen der Bundesdruckerei



Teaser: cognitix Threat Defender



Teaser: cognitix Threat Defender

genua Ein Unternehmen der Bundesdruckerei

genua

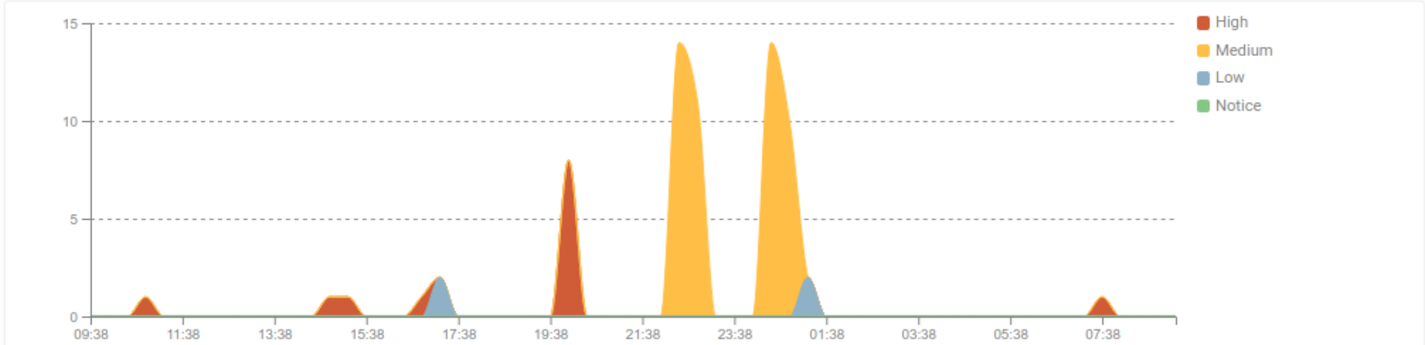
APPLY

- Analytics
- Policy
- Assets
- Threat Intelligence
- Network
- Logging
- Settings
- Diagnostics
- Documentation
- Support
- About
- Sign Out
- Collapse Menu

Incident Logs | Intelligence Database

Actions | Create Logs (Last 24 h) | Create Logs (Last Week) | Create Logs (Last Month) | Create IPS (Last 24 h) | Create IPS (Last Week) | Create IPS (Last Month) | Create IoC (Last 24 h) | Create IoC (Last Week) | Create IoC (Last Month)

Incidents within the last 24 hours



Incident Logs

time	high	medium	low	notice
Last Month	41	152	24	5
Last 6 Months	41	152	24	5
Last Week	40	152	24	5
Last Day	13	49	4	0
Last Hour	0	0	0	0

SEARCH

Page Size: 50

Created At	Se...	Action	Rule	Indicator	Classi...	Assets	IP Addresses	Por...	Countries
2019.09.06 - 09:38		→ allow	IPS severity info	EICAR pattern	HTTP	nuc-sven	10.10.0.181 [b8aeed78d364.hq.packetwe 213.211.198.58	35628 80	Unknown or Invalid Territory Germany
2019.09.06 - 07:52		→ allow	IPS severity high	ET TROJAN Backdoor family PCRat/Gh0st CnC traffi	TCP	asset-68847e694b39	10.10.0.147 80.154.94.10 [gg-0.genua.de]	28958 1022	Unknown or Invalid Territory Germany
2019.09.06 - 01:35		→ allow	IPS severity low	ET POLICY GNU/Linux APT User-Agent Outbound like	HTTP	robot-runner-4	10.10.10.107 [robot-runner-4.hq.packetwe 2.18.232.55	59060 80	Unknown or Invalid Territory Unknown or Invalid Territory
2019.09.06 - 01:35		→ allow	IPS severity low	ET POLICY GNU/Linux APT User-Agent Outbound like	HTTP	robot-runner-4	10.10.10.107 [robot-runner-4.hq.packetwe 91.189.95.83 [haetae.canonical.com]	43506 80	Unknown or Invalid Territory United Kingdom
2019.09.06 - 01:07		→ allow	IPS severity medium	ET POLICY curl User-Agent Outbound	HTTP	robot-runner-4	10.10.10.107 [robot-runner-4.hq.packetwe 213.211.198.62	36146 80	Unknown or Invalid Territory Germany
2019.09.06 - 01:06		→ allow	IPS severity medium	ET POLICY curl User-Agent Outbound	HTTP	robot-runner-4	10.10.10.107 [robot-runner-4.hq.packetwe 213.211.198.62	36144 80	Unknown or Invalid Territory Germany
2019.09.06 - 01:05		→ allow	IPS severity medium	ET POLICY curl User-Agent Outbound	HTTP	robot-runner-4	10.10.10.107 [robot-runner-4.hq.packetwe 213.211.198.62	36142 80	Unknown or Invalid Territory Germany
2019.09.06 - 01:03		→ allow	IPS severity medium	ET POLICY curl User-Agent Outbound	HTTP	robot-runner-4	10.10.10.107 [robot-runner-4.hq.packetwe 213.211.198.62	36132 80	Unknown or Invalid Territory Germany
2019.09.06 - 01:03		→ allow	IPS severity medium	ET POLICY curl User-Agent Outbound	HTTP	robot-runner-4	10.10.10.107 [robot-runner-4.hq.packetwe 213.211.198.62	36130 80	Unknown or Invalid Territory Germany