Microsoft

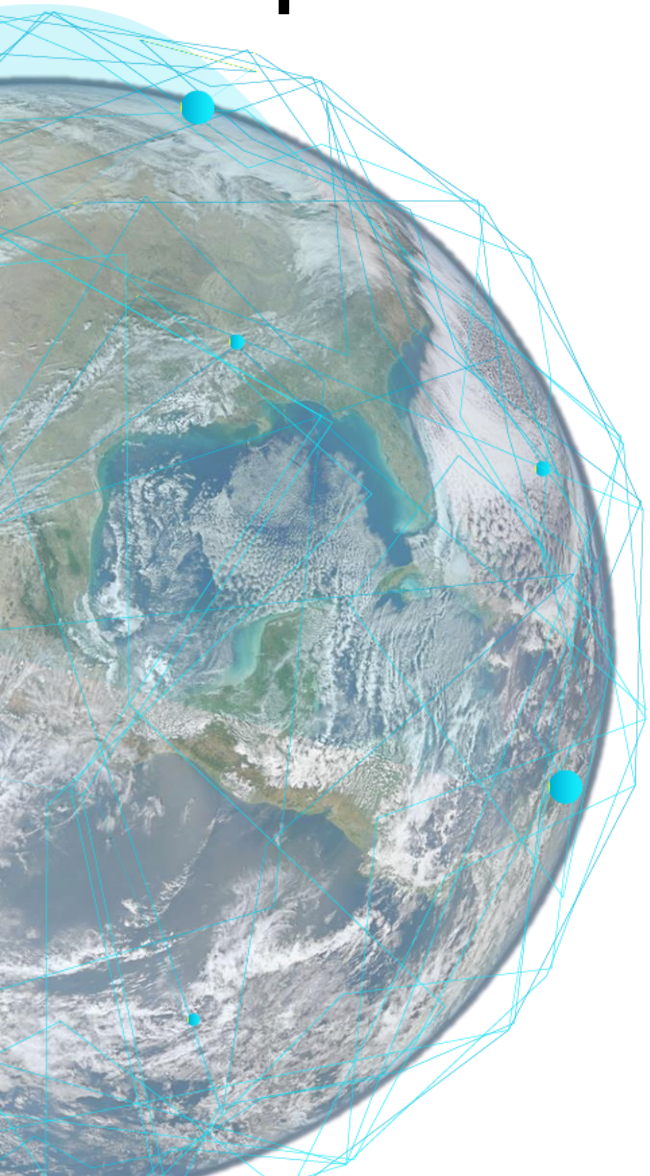
IT Security – „post-pandemisch“

(optimistische) Gedanken zur aktuellen Sicherheitslandschaft

Michael Wirth
CISSP, CISA, CIPP
Cloud Solution Architect, Customer Architecture & Engineering
Microsoft Corporation

May-30

Komplexität



Geschwindigkeit

23% aller Empfänger öffnen Phishing Mails

50% davon öffnen und klicken Anhänge innerhalb der ersten Stunde

24 Stunden dauert es vom Click bis zur Kompromittierung der Domäne

Volumen

18K neue Schwachstellen pro Jahr (2021)

50% Aller neuen Schwachstellen werden als kritisch bewertet

100K Alarme pro Tag

Agenda – worüber sprechen wir heute?

- Die Auswirkungen der Pandemie
- Geo-Politik und neue Risiken
- Supply Chain
- Bedrohung durch Ransomware
- Was muss IT Security heute leisten?

Optimism is a strategy for making a better future. Because unless you believe that the future can be better, you are unlikely to step up and take responsibility for making it so.

Noam Chomsky

We've seen two years' worth of digital transformation in two months."
—Satya Nadella, Microsoft CEO

2022

Home Office

Europa

Metaverse

Zero Trust

Energie- und Rohstoffkosten

Souveränität

Wir werden nicht komplett zum vorherigen Modell zurückkehren

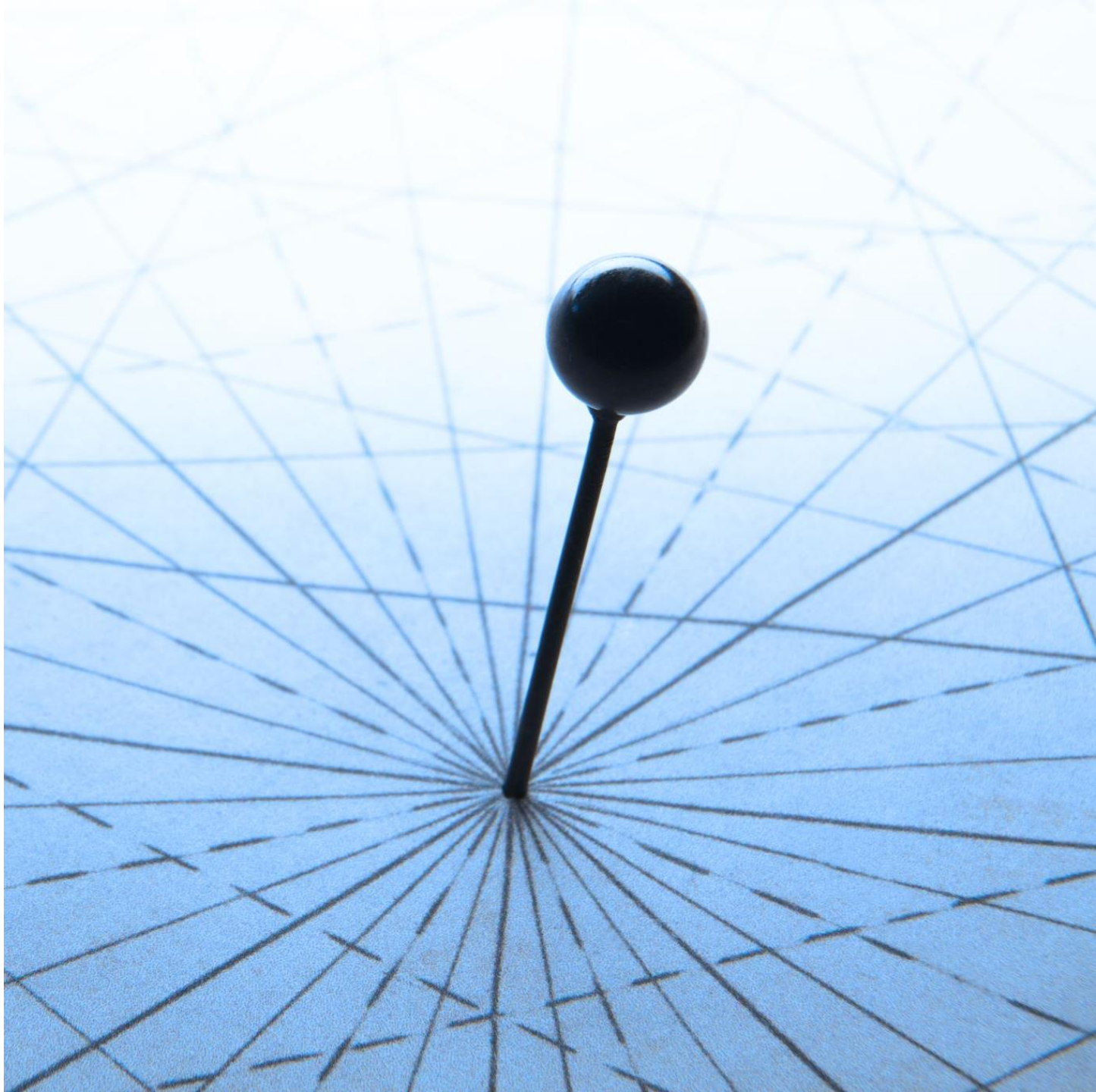
Schöne neue Welt? – diese Trends *waren* bereits da

~~User sind Mitarbeiter~~		Mitarbeiter, Partner, Kunden, Bots
~~Endgeräte von der Firma verwaltet~~		“Bring Your Own Device” und IoT
~~Anwendungen laufen on-premises~~		Aufstieg der Cloud Anwendungen
~~Monolithische Apps~~		Micro Services, Public RESTful APIs
~~Corpnet und Firewalls~~		Erodierende Perimeter
~~Packet tracking und Logs lokal~~		Rapides Wachstum im Signalvolumen

Dimensionen jenseits von Zero Trust & Access Control

- Bedrohungen im Security Operations Center (SOC) erkennen und darauf reagieren
- Daten unabhängig vom Ablageort überall schützen
- Durchgehende Bewertung und Verbesserung der “IT infrastructure security posture”.
- Integrieren von Sicherheit in den Application Development Process
- Permanentes Aufspüren und Mitigieren von Compliance-Risiken
- Erweiterte Anwendung über IoT und Operational Technology (OT) Assets hinaus.

Geo-Politik



Human Operated Ransomware

HUMOR ist…

…das Akronym für **Human** **O**perated **R**ansomware

Commodity Ransomware

- → Ziel sind **einzelne** Personen oder Maschinen
- → **Vorgefertigte Angriffsroutinen** / best-effort
- → **Opportunistische** Verschlüsselung
- → Für sich genommen keine Katastrophe
- → Beste Verteidigung: wie bei **Malware-Bekämpfung**

Human Operated Ransomware

- → Ziel ist ein **ganzes Unternehmen**
- → Angepasste Angriffe, die von einem **entschlossenen menschlichen Gegner** geplant sind
- → **Vorgeplante** Daten-Verschlüsselung und Exfiltration
- → Will eine **massive** and **visible** Schädigung des Geschäftsbetriebs verursachen
- → Beste Verteidigung: **“eviction” des Angreifers**

Gegenmaßnahmen (Nichts wirklich Neues)

1. Wiederherstellung, bzw. die Fähigkeit dazu, aber auf traditioneller Informationsschutz durch Verschlüsselung, etc.
2. Einschränkung des Wirkungskreises (Least privilege, bzw. Schutz der privilegierten Anwender)
3. Schutz vor dem Eindringen der Angreifer (Identity, Access, Endpoints…)

Die Priorisierung ist möglicherweise neu, da es primär darum geht, das „Geschäftsmodell“ der Angereifer zu stören

Choose to be optimistic, it feels better.

Dalai Lama

Supply Chain

- Sicherheit *bei* den Zulieferern und Partnern
  - Endgeräte, Nutzerkonten, Authentifizierungsmethoden
  - Audit?
- Software Supply Chain selbst
  - Beispiele: Solarwinds, aber auch Log4j und zlib
- Microsoft
  - SoNic (https://github.com/sonic-net/SONiC), Mu (https://microsoft.github.io/mu)
  - Software-Bills-of-Materials https://devblogs.microsoft.com/engineering-at-microsoft/generating-software-bills-of-materials-sboms-with-spdx-at-microsoft/
- Open Source

> I am not an optimist. I'm a very serious possibilist. It's a new category where we take emotion apart and we just work analytically with the world.
>
> Hans Rosling

“Fragen zum Mitnehmen”: Wie sieht moderne IT Security für Unternehmen heute idealerweise aus?

- Wer kann wirklich von überall arbeiten?
- Wie lange dauert es, einem neuen Geschäftspartner Zugang zu einer eigenen Anwendung zu geben?
- Wie schnell kann man einem Nutzer den effektiven Zugriff entziehen? 60 min?
- Wie agil sind wir? Und wie benutzerfreundlich?
- Wie gehen wir mit hoch-privilegierten Konten um?
- Wieviel Legacy steht rum?
- Haben wir einen „Incident Response“-Plan?
- Wie schnell können wir bei Totalschaden recovern?

We would accomplish many more things if we did not think of them as impossible.

Vince Lombardi

Read more!

- Microsoft Digital Defense Report: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
- Microsoft über Compromise Recovery: https://www.microsoft.com/security/blog/2022/04/04/microsoft-crsp-shares-the-ways-human-behavior-affects-compromise-recovery/
- Human Operated Ransomware: https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware
- Mark Simos zu Zero Trust: https://www.microsoft.com/security/blog/2022/04/14/a-clearer-lens-on-zero-trust-security-strategy-part-1/
- Roger Halbheer über "Exposed Environments": https://www.linkedin.com/smart-links/AQGbMjRe-br2bA/5372b730-b041-4f76-bd56-1e11b5bf8783 und Microsoft Artikel: https://www.microsoft.com/de-de/techwiese/cybersecurity/default.aspx
- BSI Maßnahmenkatalog Ransomware: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.html
- Für mehr Grund zum Optimismus: Hans Rosling, Factfulness (ISBN 9127163288)

Be kind whenever possible. It is always possible.

Dalai Lama