Paradigmenwechsel in der IT-Sicherheit

Never trust, always verify: Zero-Trust Framework Microsoft 365

Frank
Siepmann
Manager, Technical Services

Frank.Siepmann@tdsynnex.com
+49 175 7270438

TD SYNNEX

Kistlerhofstraße 75
Munich, Bavaria 81379
Germany

www.tdsynnex.com

Modernes Arbeiten ist jetzt hybrides Arbeiten

TD SYNNEX

Hybrides Arbeiten

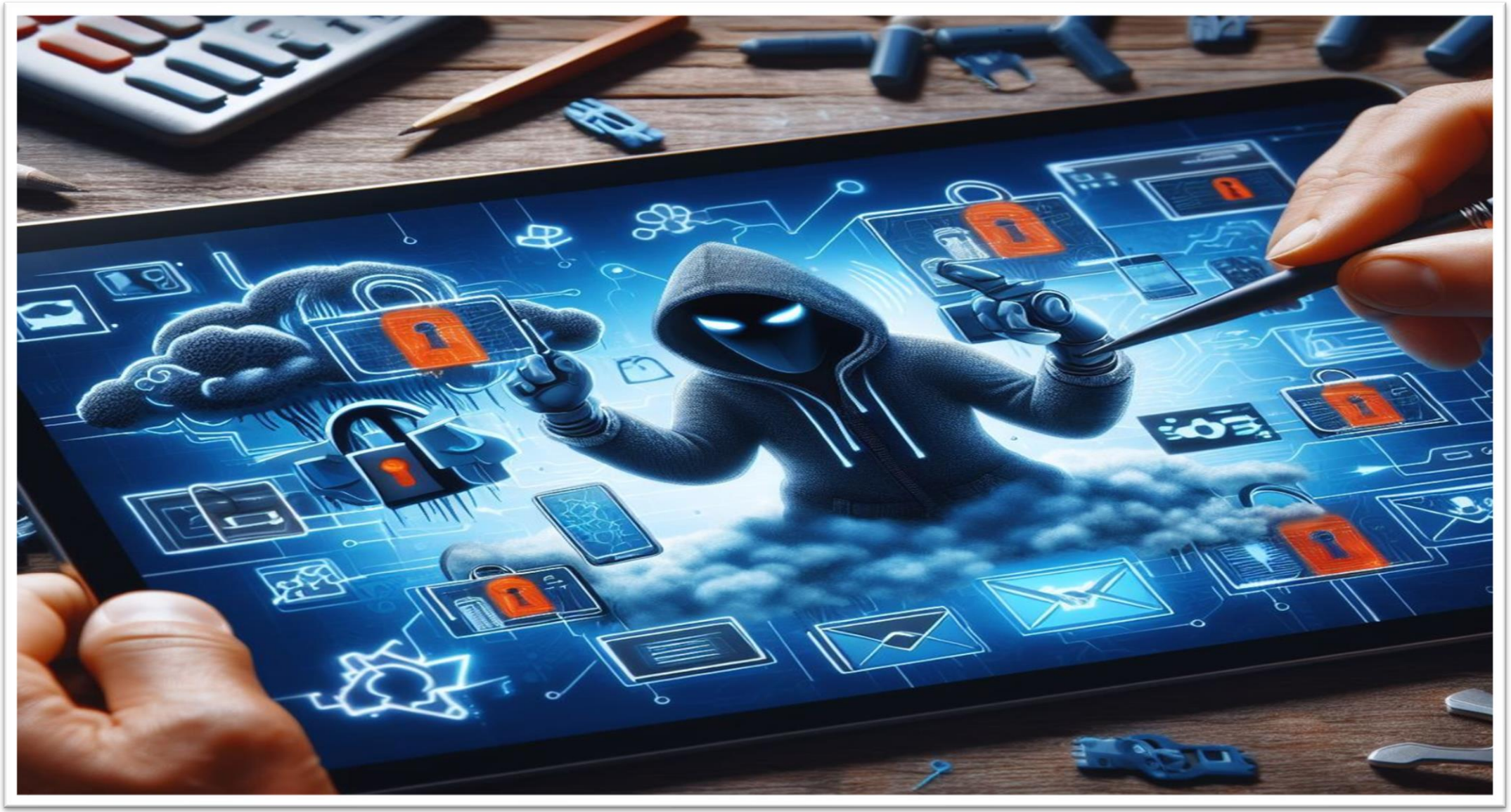
TD SYNNEX

Mythen und ihre Fakten

Cyberangriffe häufen sich immer mehr.
Die Angriffsfläche vergrößert sich durch die fortschreitende Digitalisierung ebenso. Dabei müssen IT-Abteilungen und Experten mithalten können. Das wird durch Mythen und Missverständnisse jedoch nur erschwert.

„The Dark Side“ – Motivation, Angriffsvektoren, Angriffsbeispiele

TD SYNNEX



Motivation eines Bad Actors?

Kategorie	Produkt	Durchschnittlicher Dark Web Preis (USD)
Kreditkartendaten	Kreditkartendaten, Kontostand bis 5.000 $	$ 120
	Geklonte VISA/Mastercard mit PIN	$ 20
Zahlungsabwicklungsdienste	PayPal-Kontodaten, Mindestguthaben 1.000 $	$ 20
	50 gehackte PayPal-Konto-Logins	$ 150
Krypto-Konten	USA verifiziertes LocalBitcoins-Konto	$ 120
Soziale Medien	Gehacktes Facebook-Konto	$ 45
Gefälschte Dokumente	Personalausweis der Europäischen Union	$ 160

Gängige Bedrohungen

Datenpanne

Inklusive:

- Phishing
- Spear-Phishing
- Tech-Support-Betrug
- Einschleusung von SQL-Befehlen
- Malware zum Ausspähen von Kennwörtern und Bankinformationen

Wörterbuchangriff

Hierbei handelt es sich um eine Form von Identitätsangriffen.

Ein Hacker versucht, eine Identität zu stehlen, indem eine Vielzahl von bekannten Kennwörtern ausprobiert wird.

Wörterbuchangriffe werden auch als „Brute-Force-Angriffe“ bezeichnet.

Ransomware

Dies ist eine Form von Malware, mit der Dateien und Ordner verschlüsselt werden.

Sie zielt darauf ab, Geld von den Opfern zu erbeuten.

Störangriffe

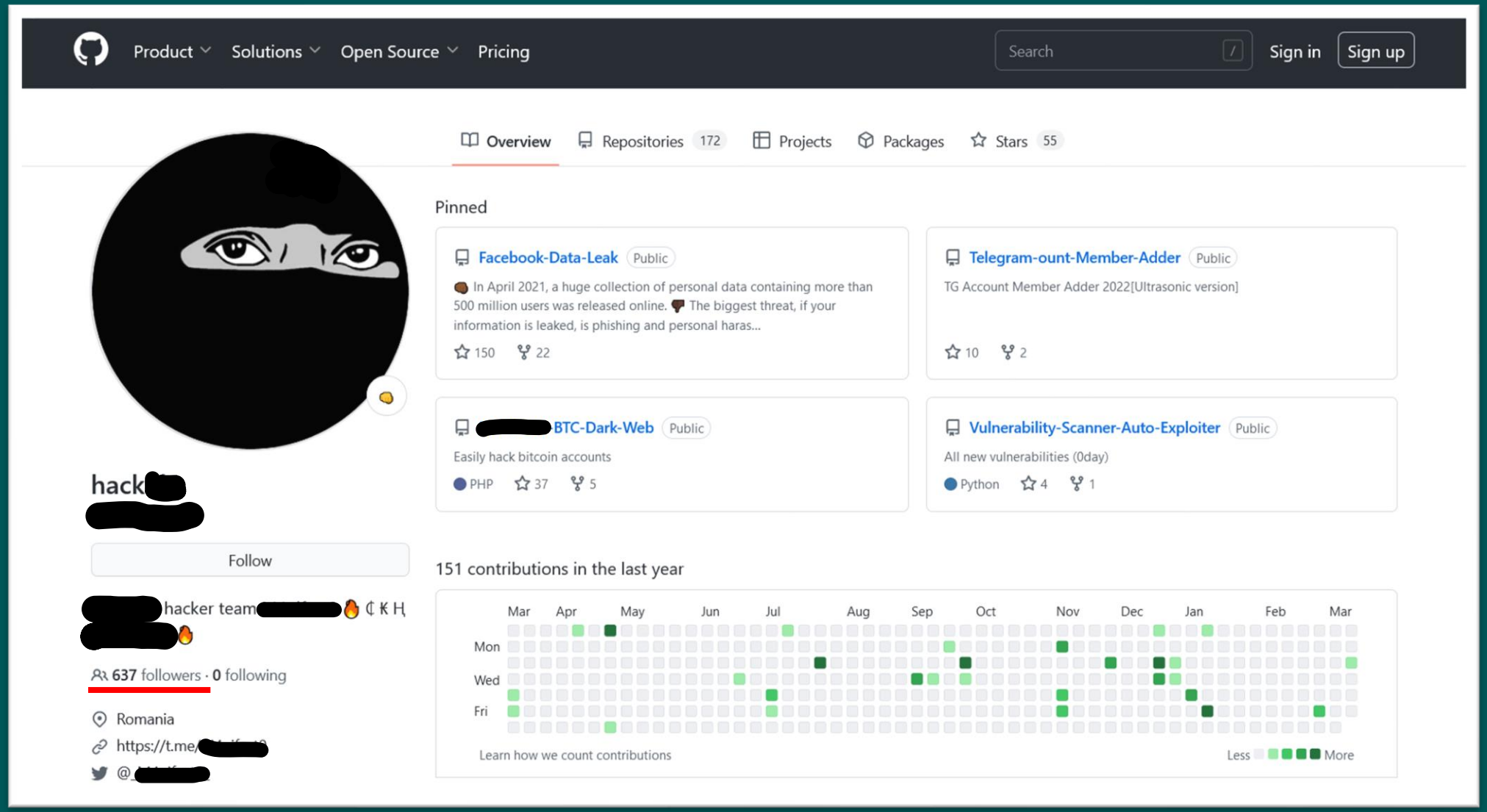
Ein verteilter Denial-of-Service-Angriff (DDoS) zielt darauf ab, die Ressourcen einer Anwendung auszuschöpfen.

DDoS-Angriffe können jeden Endpunkt zum Ziel haben.

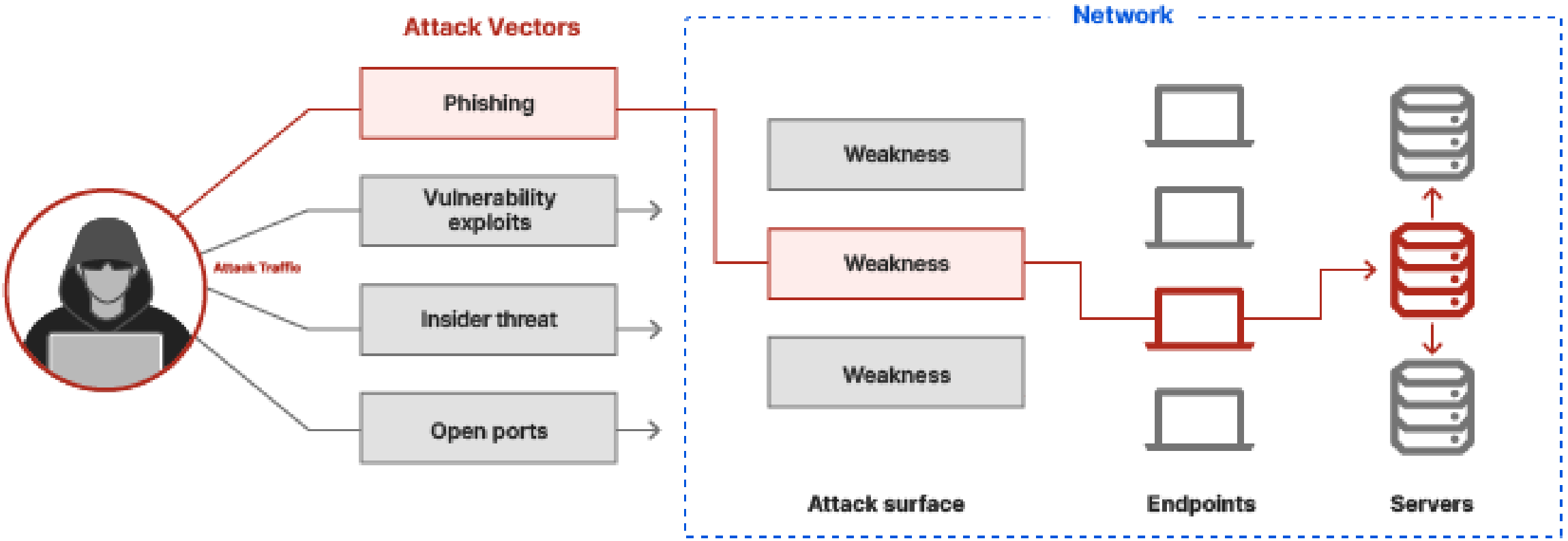
Andere gängige Bedrohungen sind Coinminer, Rootkits, Trojaner, Würmer sowie Exploits und Exploitkits.

TD SYNNEX

Hacking Repositories – Clearweb!

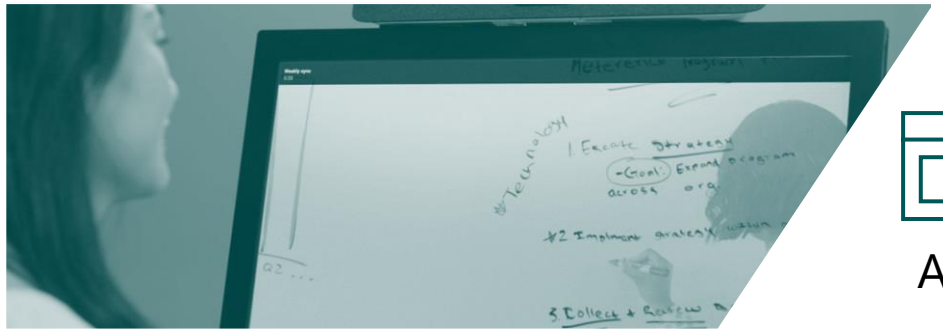


Angriffsvektor



TD SYNNEX

Zero Trust über den gesamten digitalen Bestand hinweg



Identität

Apps

Daten

Geräte

Netzwerk

Infrastruktur

Personenebene

Digitale Ebene

Physische Ebene

VON

AN

TD SYNNEX

„Alte Welt“ Implicit Trust

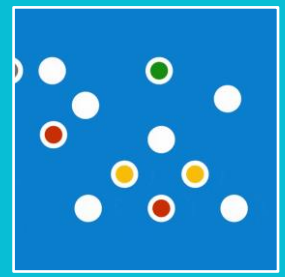
Schutz durch Unternehmens-Firewall

Sicherheitsanomalien werden geprüft

Modernes Arbeiten nur bedingt möglich

„Hybride Welt“ Zero Trust

Vielzahl an Endgeräten



Mobiles Arbeiten an jedem beliebigen Ort
(produktiv & sicher)

Vernetzte Welt

Microsoft Zero-Trust-Prinzipien
Leitfaden für die technische Architektur

TD SYNNEX

Explizit verifizieren

Überprüfen Sie **immer alle verfügbaren Datenpunkte**, einschließlich

- Benutzeridentität und Standort
- Gerätezustand
- Dienst- oder Workloadkontext
- Datenklassifizierung
- Anomalien

Verwenden des Zugriffs nach dem Prinzip der geringsten Rechte

Um sowohl Daten als auch Produktivität zu sichern, beschränken Sie den Benutzerzugriff mithilfe von

- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors

Verstoß annehmen

Minimieren Sie den „Explosionsradius“ bei Verletzungen / Einbrüchen und verhindern Sie die Ausbreitung durch

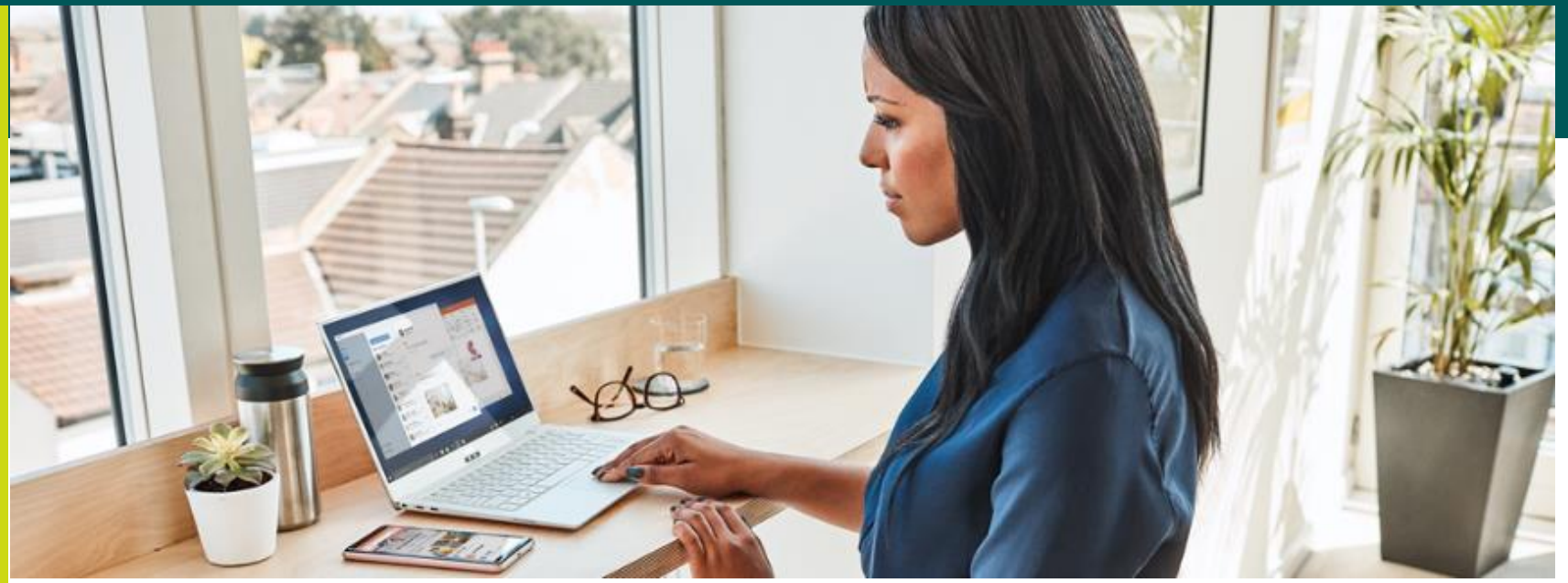
- **Segmentierung** des Zugriffs nach Netzwerk, Benutzer, Geräten und App-Bewusstsein.
- **Verschlüsselung** aller Sitzungen Ende-zu-Ende.
- Nutzen Sie **Analysen** zur Erkennung von Bedrohungen, zur Transparenz der Haltung und zur Verbesserung der Abwehr

Authentifizierung

Verwenden Sie intelligente Schutzrichtlinien und Risikobewertungen, um Bedrohungen zu blockieren.

81%

aller Hacks durch gestohlene oder schwache Passwörter



Microsoft Authenticator

Windows Hello

FIDO2 Security key

Push Notification

Soft Tokens OTP

Hard Tokens OTP

SMS, Voice

Multi-Faktor-Authentifizierung verhindert 99,9% der Identitätsangriffe.

Phishing mittels Punycode-Domains

https://www.bsı.bund.de/Login/Login/login_node.html?rid=J2jCQjM

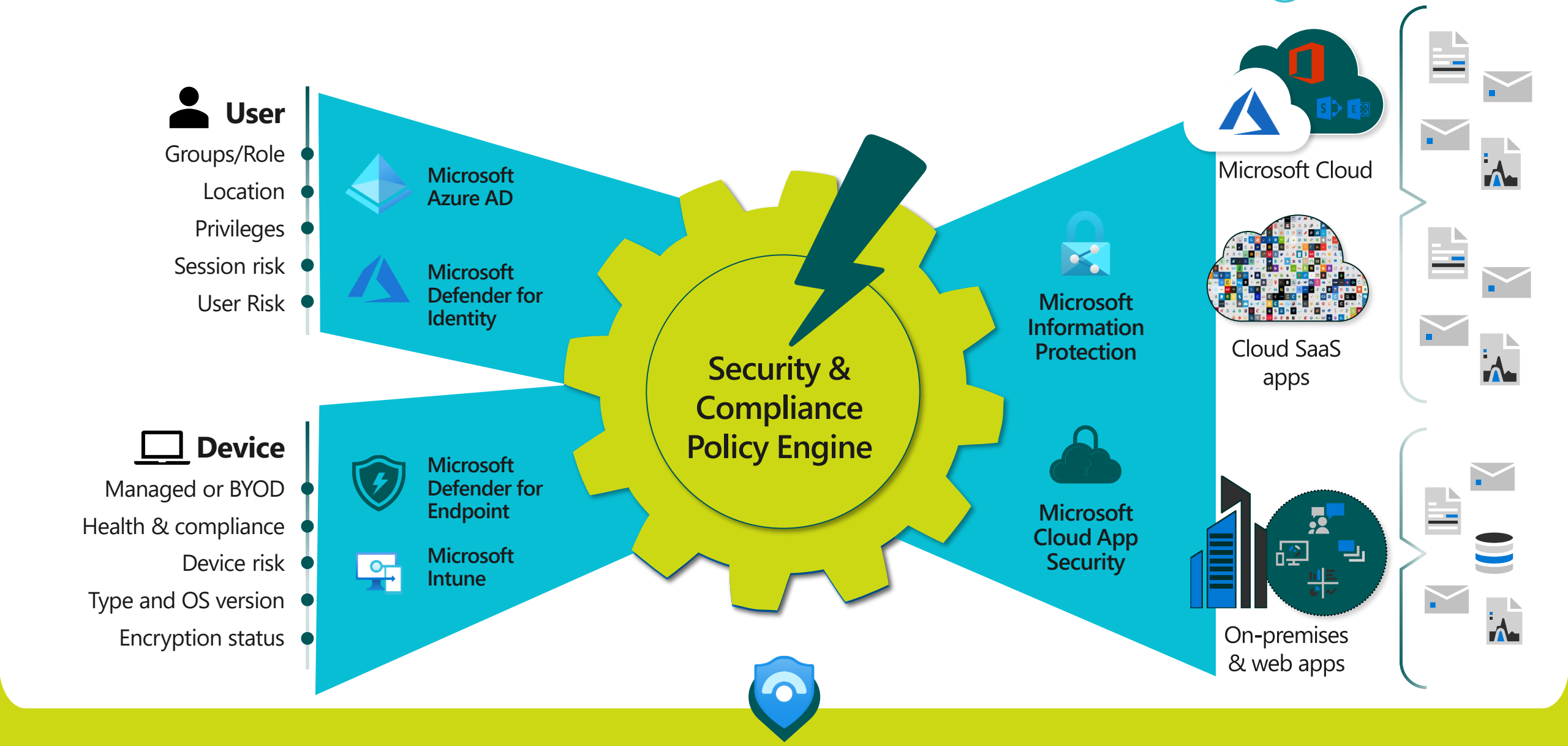
https://www.bsi.bund.de/Login/Login/login_node.html

Welche Domain ist korrekt?
https://www.apple.com/
https://www.apple.com/

Confusable	Confused With
CYRILLIC SMALL LETTER A а	LATIN SMALL LETTER A a
CYRILLIC SMALL LETTER O о	LATIN SMALL LETTER O o
CYRILLIC SMALL LETTER ER р	LATIN SMALL LETTER P p
CYRILLIC SMALL LETTER IE е	LATIN SMALL LETTER E e
LATIN SMALL LETTER DOTLESS I ı	LATIN SMALL LETTER I i
LATIN SMALL LIGATURE OE œ	LATIN SMALL LETTER O/LATIN SMALL LETTER E oe

Verwenden Sie das Microsoft Zero Trust Modell

TD SYNNEX



Vielen Dank und bleiben Sie sicher!