Mbuf Security Spotlight

Tipps und Tricks zur Absicherung Ihrer hybriden IT-Umgebung

Net at Work
Building IT-Excellence.

Experten für die beste Lösung von allen: Ihre maßgeschneiderte.

Thomas
Welslau

Senior Consultant Modern Workplace

Frank
Carius

Enterprise Architekt

Net at Work

130+ Mitarbeiter
Gründungsjahr: 1995
Standort: Paderborn

Gold
Microsoft Partner
Cloud Productivity
Microsoft

Systemintegrator mit Lösungen und Werkzeugen für die digitale Kommunikation und Zusammenarbeit

Lage der IT-Sicherheit

BSI – Die Lage der IT-Sicherheit in Deutschland 2021

- „IT-Sicherheitslage bleibt angespannt bis kritisch“
- „So bringt die Digitalisierung mit all ihren Chancen und Möglichkeiten auch viele Gefahren und eine wachsende Angriffsfläche mit sich“

Microsoft Digital Defense Report

- “Identity and password/phishing attacks are cheap, and on the rise. Why would an attacker break in when they can log in?”
- “Phishing is the most common type of malicious email observed in our threat signals.”

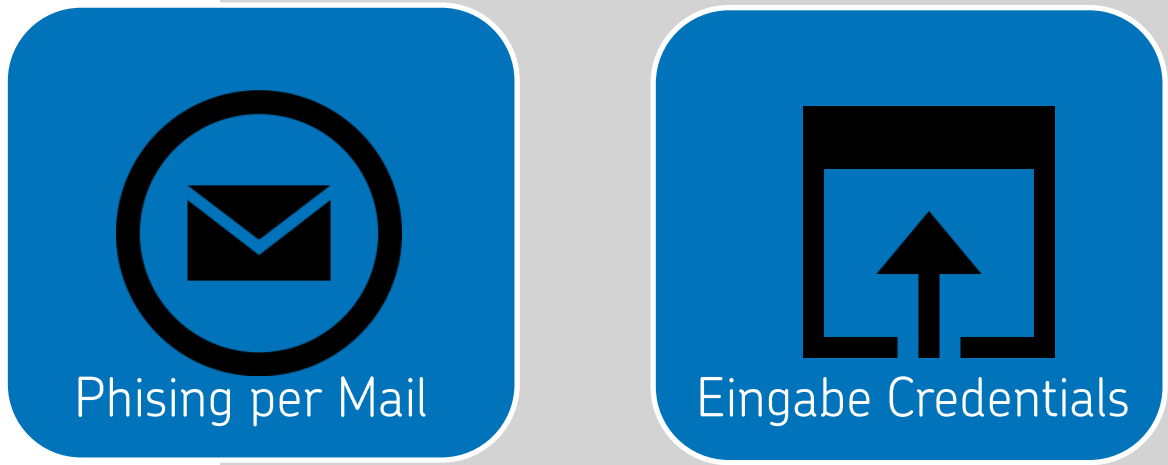
Erfahrungen – Credential Phising

Vorgehen:

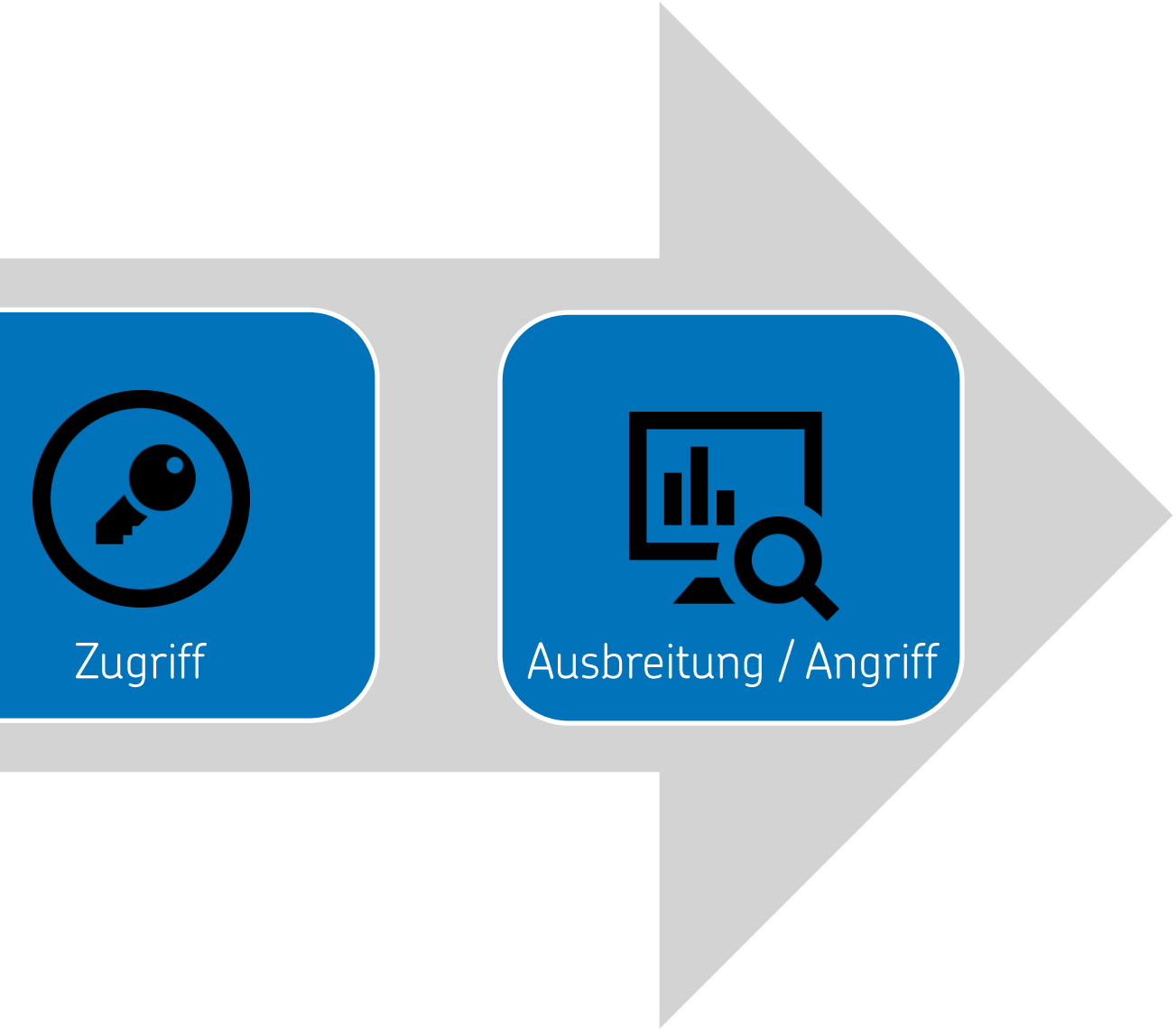
- Oftmals versenden von Mails mit URLs
- Benutzer wird zur Phishing Website umgeleitet
- Anmeldedaten werden abgefangen und zum Login verwendet

Genutzte Schnittstellen:

- Login in das E-Mail Postfach
- Zugriff per VPN
- Zugriff per Remote Desktop
- Exchange Web Services
- Warten auf neue Sicherheitslücken



Erfahrungen – Credential Phising



Verursachter Schaden

- Kerberos Golden Ticket
- Ausleiten von Daten
- Fälschen von Daten
- Verschlüsselung von Clients, Servern und Daten

Beseitigung

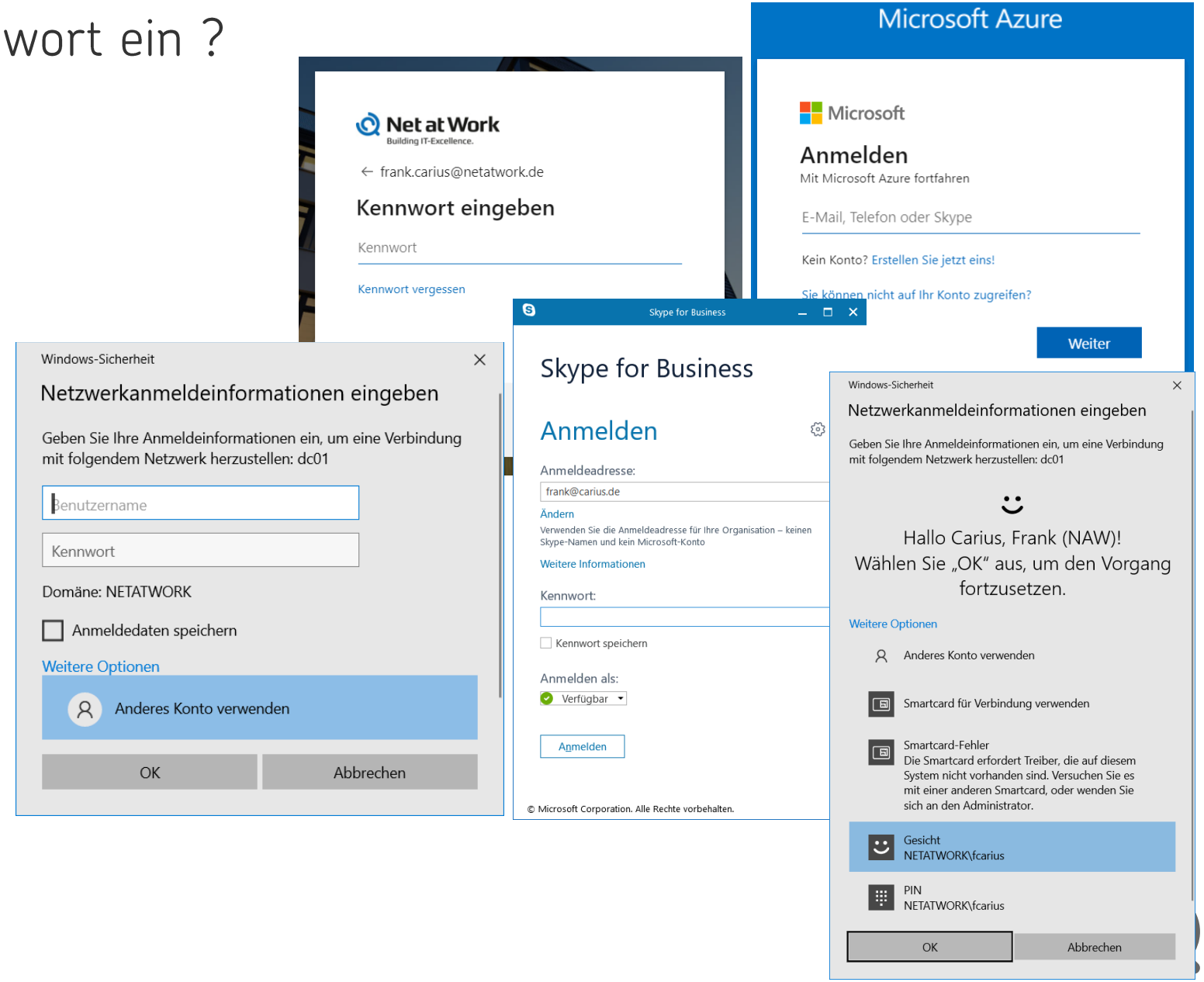
- AD Rollback/Neuaufbau
- Daten aus Backup wiederherstellen
- KDC Rollover

MediaMarkt/Saturn: Hive Ransomware erschwert Rettungsversuche durch Angriff der Backuplösungen

Wie oft geben Sie ihr Kennwort ein ?

Jeder Kennwortdialog kann falsch sein

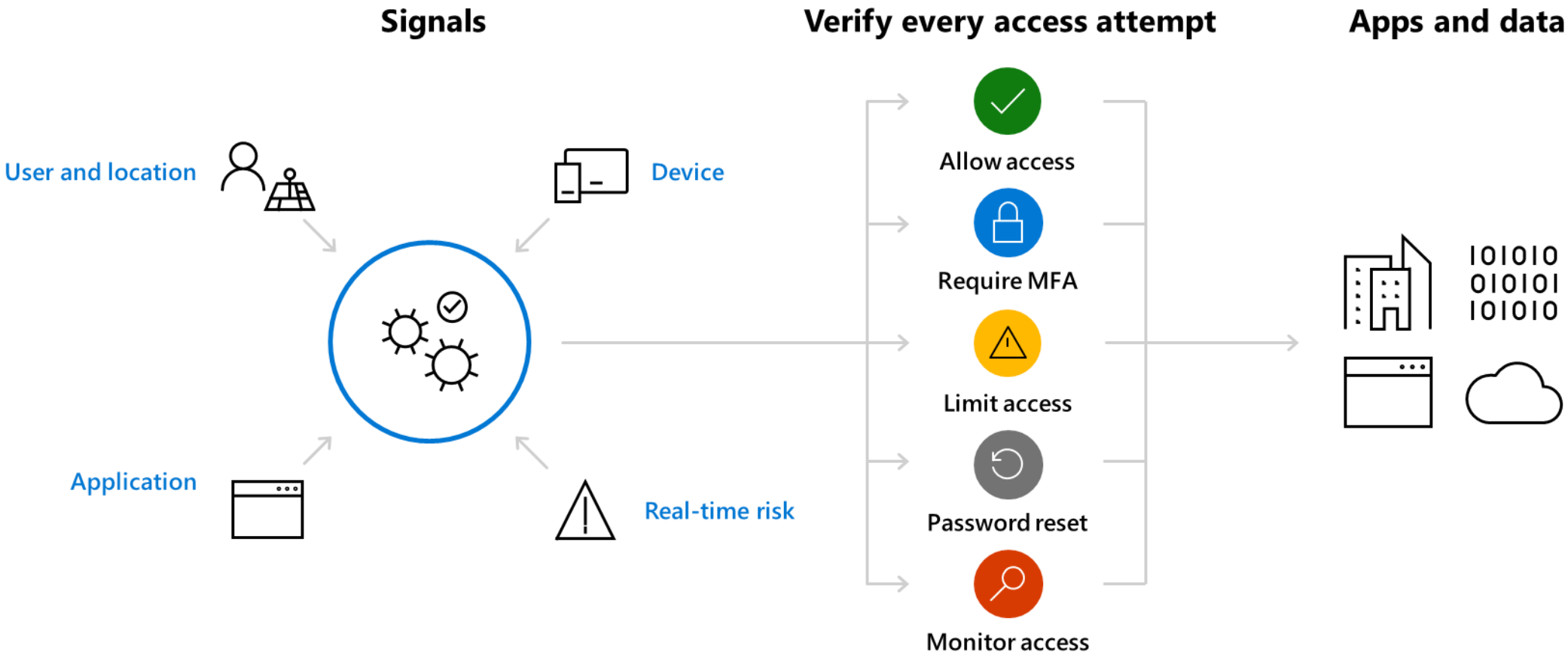
- Single SignOn
  - Kerberos, NTLM, OAUTH
- Passwordless
- Passwort nicht! regelmäßig ändern



Risiko – Einbindung von Cloud Diensten

- Cloud Dienste aus Microsoft 365 sind standardmäßig von überall erreichbar
- Passwordspraying oder Brute Force gegen die Cloud Dienste sind von überall möglich

Absicherung durch Conditional Access



Absicherung Azure AD Identity Protection

- Erweitertes Logging
- Alarmierung
- Risikoübersicht
- Reports der Anmeldungen
- Reports über privilegierte Zugriffe

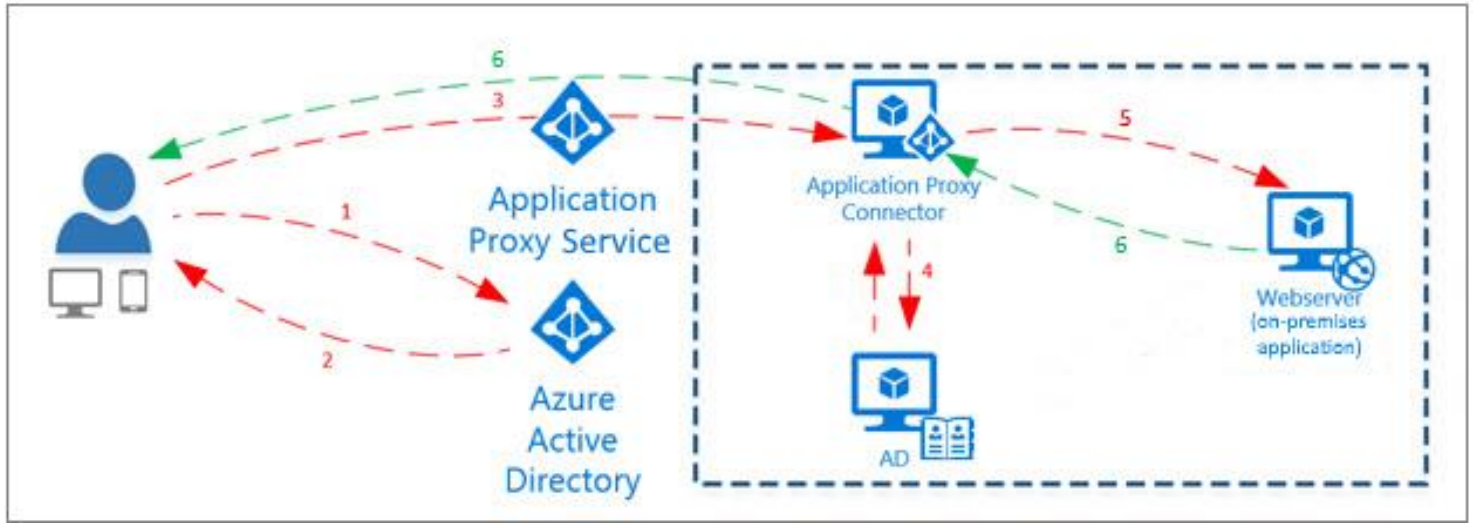
Was bedeutet Risiko?

Ungewöhnliche Anmeldeeigenschaften
Anonyme IP-Adresse
Ungewöhnlicher Ortswechsel
Mit Schadsoftware verknüpfte IP-Adresse

Absicherung **durch** hybride Infrastrukturen

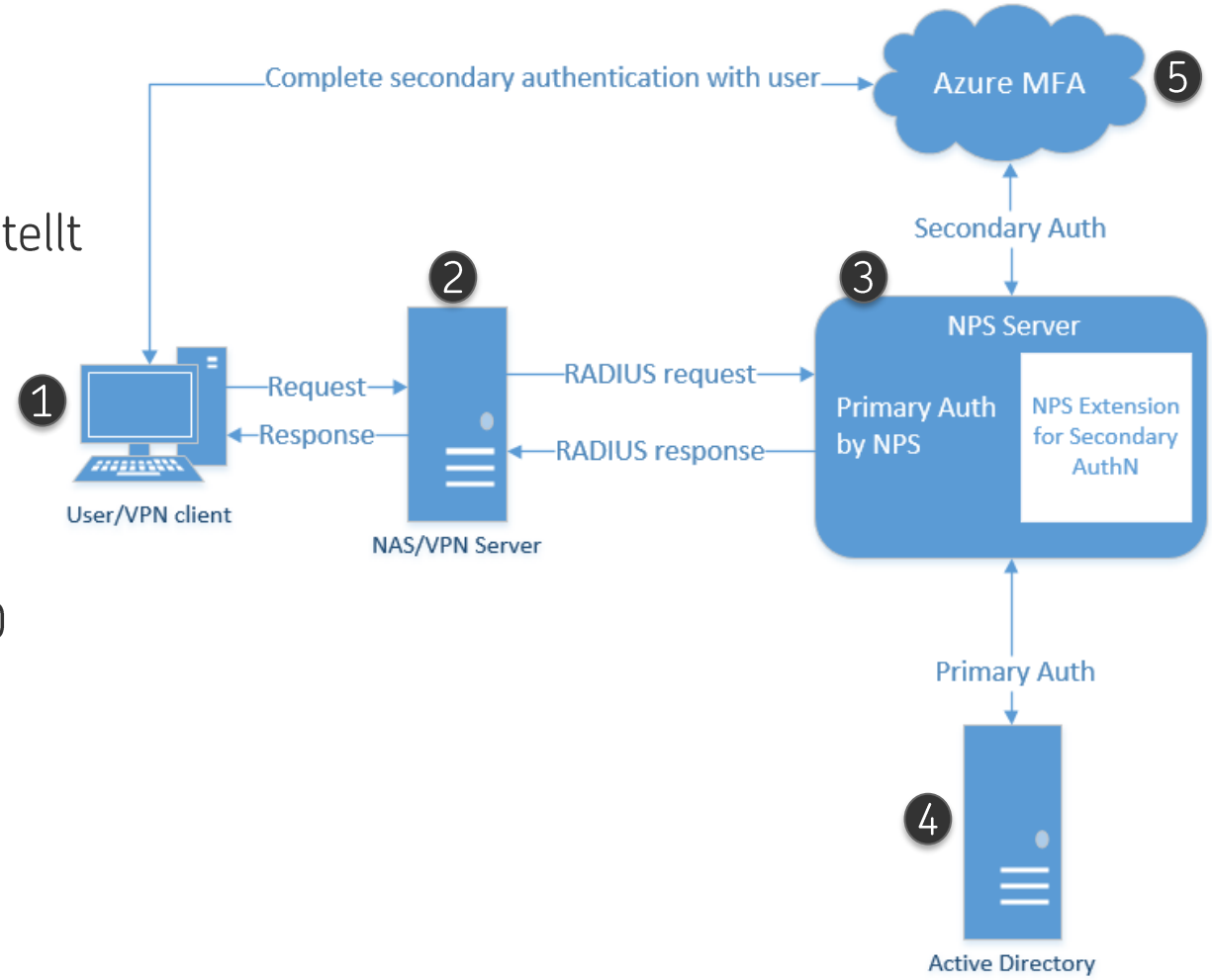
Azure AD App Proxy und MFA für lokale Dienste

- Eine ausgehende und keine eingehende Verbindung
- Keine Public-IP
- Kein öffentliches Zertifikat
- Pre-Authentifizierung
- MFA
- Conditional Access
- DDoS-Schutz
- Login Tracking
- Guest Access
- OAUTH

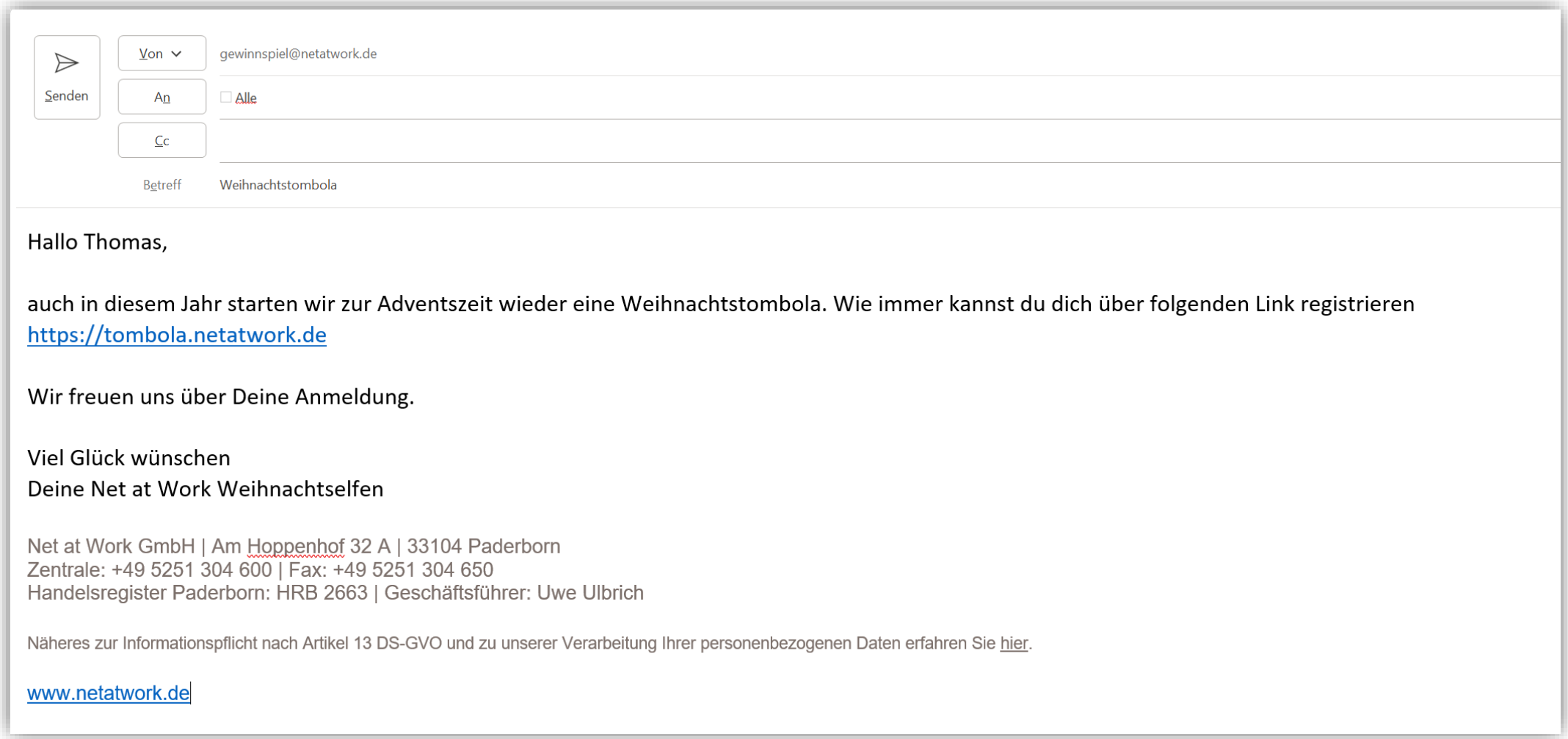


Azure MFA Radius Extension

1. Benutzer startet VPN Client
2. Verbindung mit VPN Server wird hergestellt
3. VPN Server kontaktiert RADIUS
4. Primäre Authentizierung im AD
5. Sekundäre Authentizierung im Azure AD



Phishing Mail



Senden

Von gewinnspiel@netatwork.de

An Alle

Cc

Betreff Weihnachtstombola

Hallo Thomas,

auch in diesem Jahr starten wir zur Adventszeit wieder eine Weihnachtstombola. Wie immer kannst du dich über folgenden Link registrieren
https://tombola.netatwork.de

Wir freuen uns über Deine Anmeldung.

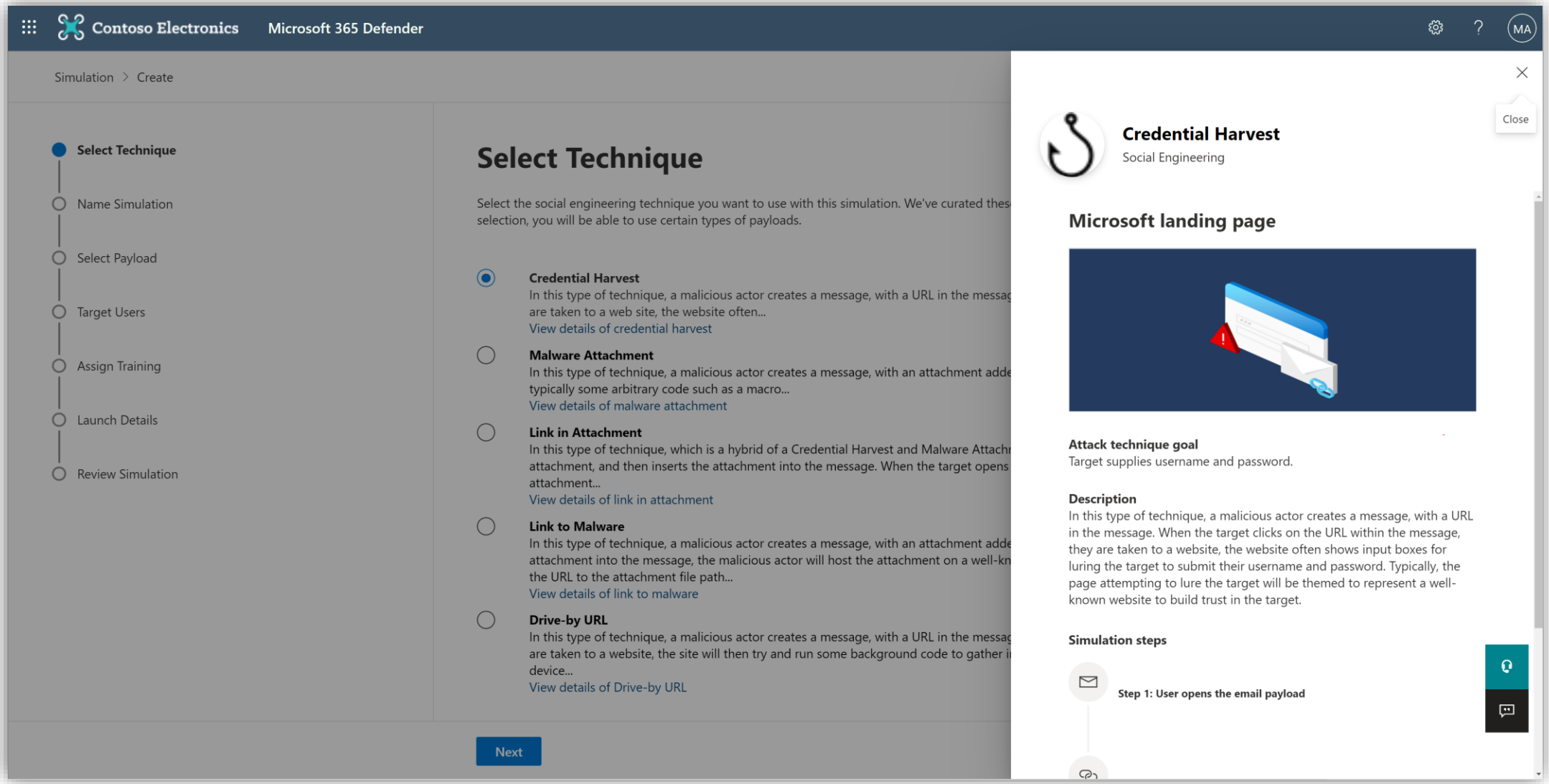
Viel Glück wünschen
Deine Net at Work Weihnachtselfen

Net at Work GmbH | Am Hoppenhof 32 A | 33104 Paderborn
Zentrale: +49 5251 304 600 | Fax: +49 5251 304 650
Handelsregister Paderborn: HRB 2663 | Geschäftsführer: Uwe Ulbrich

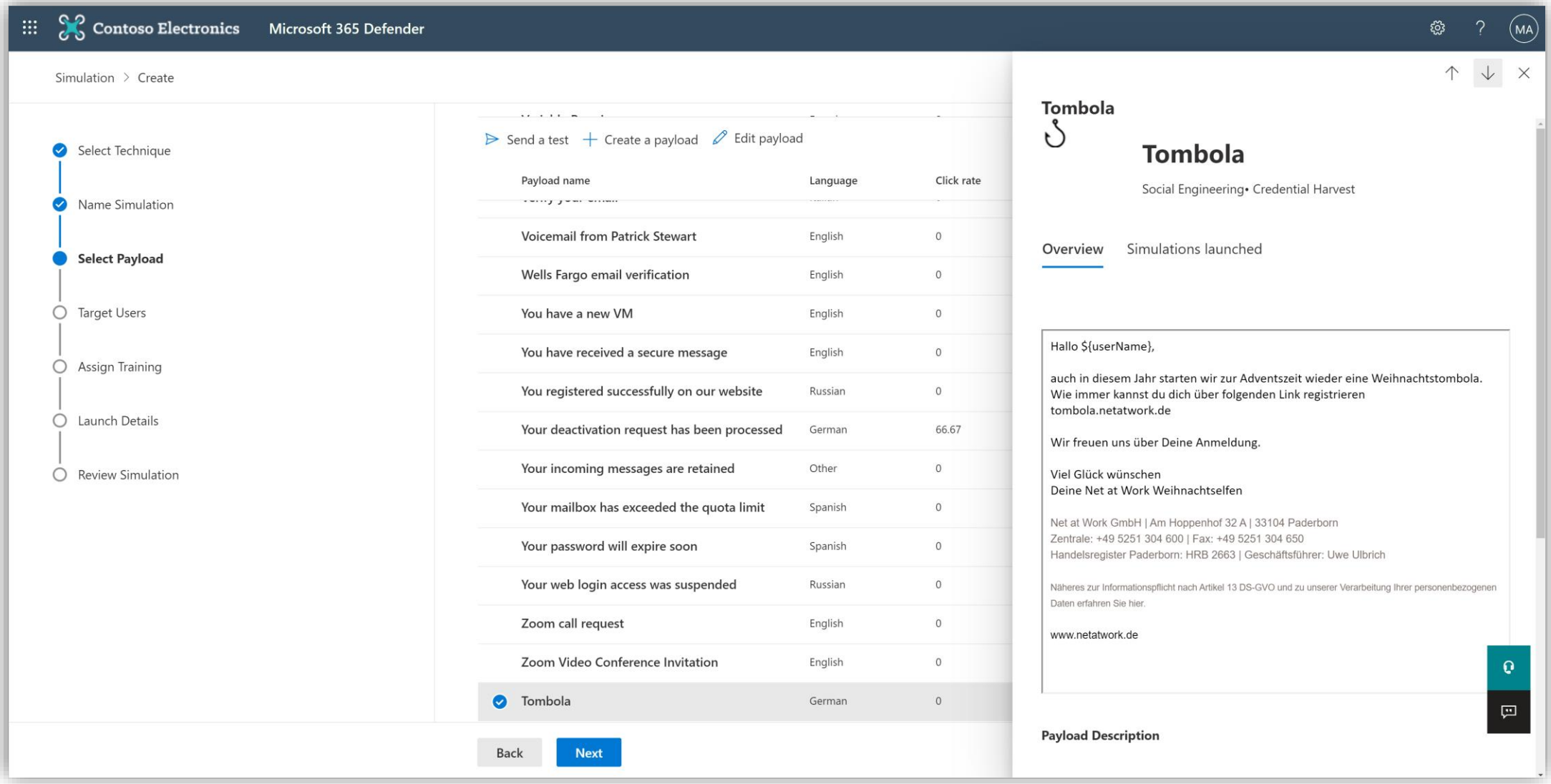
Näheres zur Informationspflicht nach Artikel 13 DS-GVO und zu unserer Verarbeitung Ihrer personenbezogenen Daten erfahren Sie hier.

www.netatwork.de

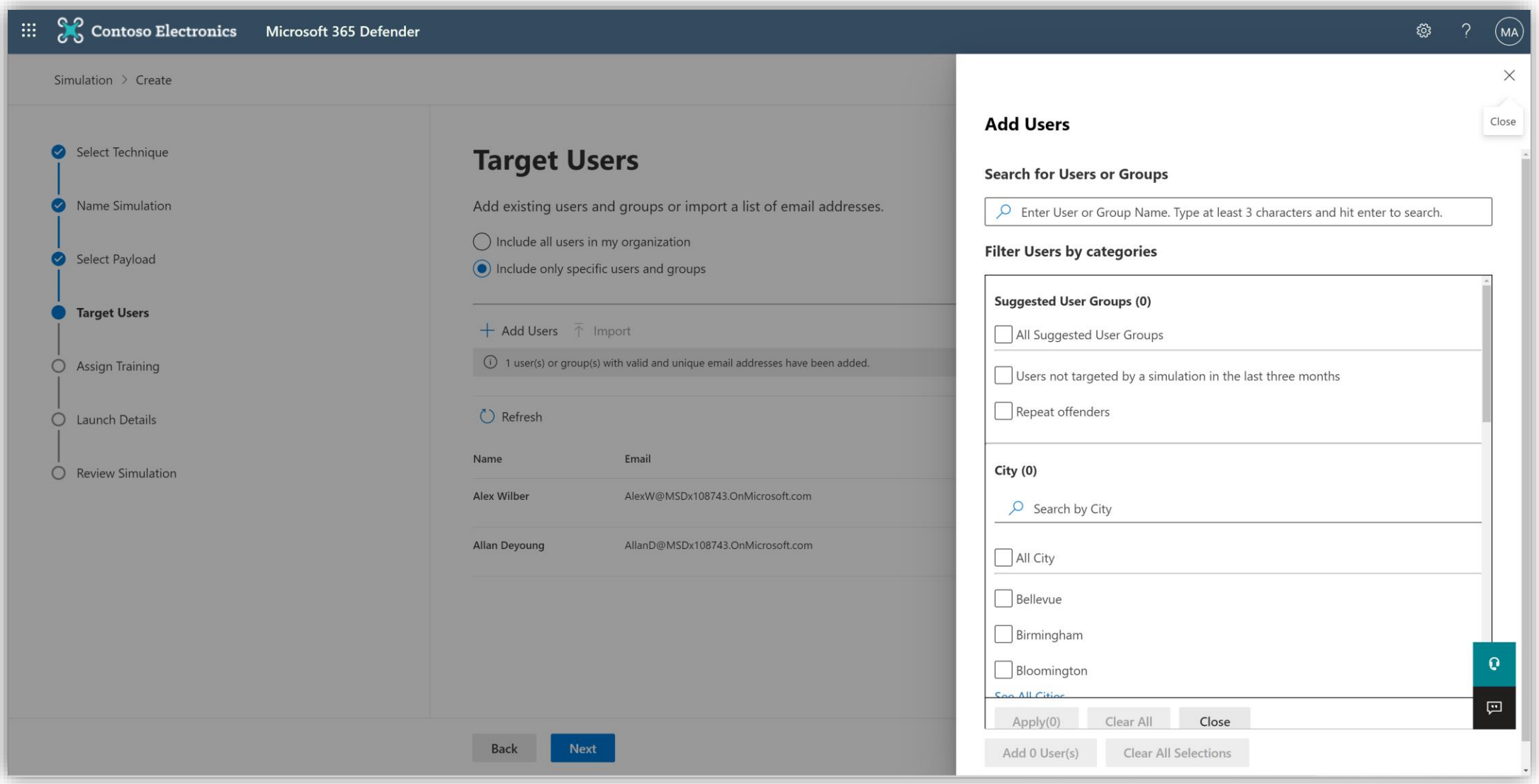
Attack Simulator – Einrichtung Phishing Mail



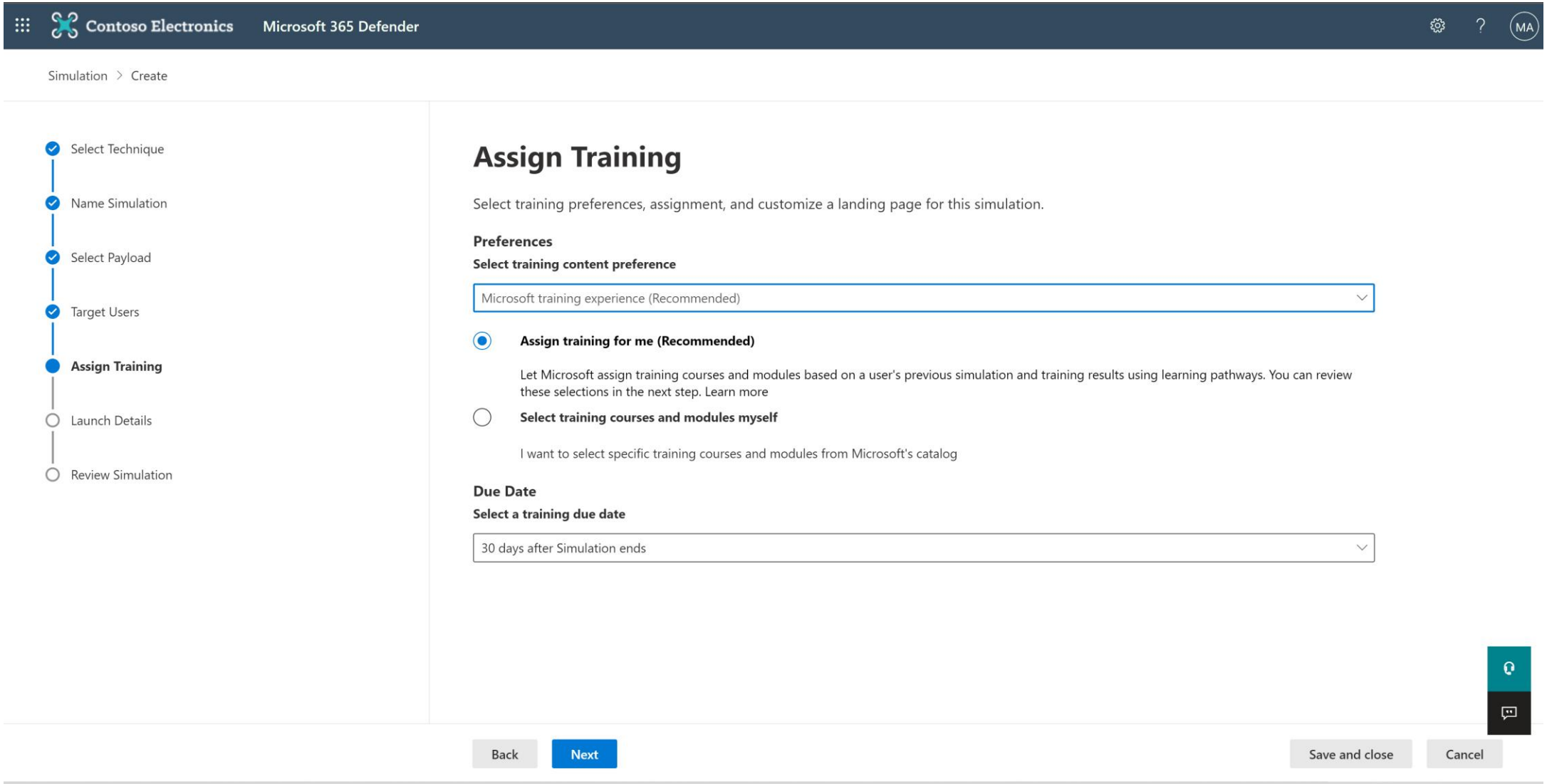
Attack Simulator – Auswahl Template



Attack Simulator - Anwenderkreis



Attack Simulator - Trainingsinhalte



Attack Simulator – Phishing Mail

Weihnachtstombola

GN

Gewinnspiel NAW <gewinnspiel@netatwork.de>
Mon 11/15/2021 8:02 AM
To: Alex Wilber

Hallo Alex Wilber,

auch in diesem Jahr starten wir zur Adventszeit wieder eine Weihnachtstombola. Wie immer kannst du dich über folgenden Link registrieren
tombola.netatwork.de

Wir freuen uns über Deine Anmeldung.

Viel Glück wünschen
Deine Net at Work Weihnachtselfen

Net at Work GmbH | Am Hoppenhof 32 A | 33104 Paderborn
Zentrale: +49 5251 304 600 | Fax: +49 5251 304 650
Handelsregister Paderborn: HRB 2663 | Geschäftsführer: Uwe Ulbrich

Näheres zur Informationspflicht nach Artikel 13 DS-GVO und zu unserer Verarbeitung Ihrer personenbezogenen Daten erfahren Sie hier.

www.netatwork.de

Reply | Forward

Attack Simulator - Benutzerhinweis

German

Alex Wilber, Sie wurden gerade von Ihrem Sicherheitsteam **gephisht.**

Kein Problem! Sie sind auch nur ein Mensch. Lassen Sie uns daraus lernen.

Anstatt Ihre Zugangsdaten wie ein Cyberkrimineller zu stehlen, haben wir Sie stattdessen auf diese Bildungsseite umgeleitet und Ihnen einige Schulungen zugewiesen.

Tipps zur Identifizierung der Phishing-E-Mail

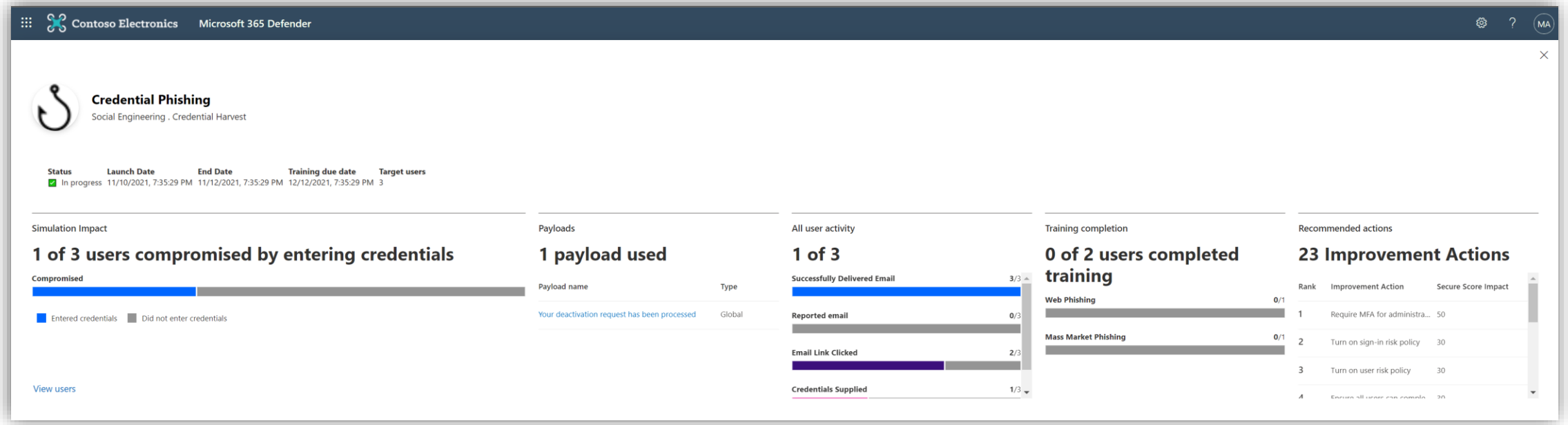
HAFTUNGSAUSSCHLUSS: Die E-Mail, auf die Sie gerade geklickt haben, ist eine Phishing-E-Mail-Simulation. Es handelt sich nicht um eine echte E-Mail des Besitzers der in der Simulation verwendeten Marke oder des Logos. Die in der Simulation aufgeführten Marken und Logos können das Eigentum ihrer jeweiligen Besitzer sein und sind in keiner Weise mit der Simulation verknüpft oder damit verbunden, noch haben die Besitzer solcher Marken und Logos die Verwendung dieser Marken und Logos in der Simulation autorisiert, gesponsert oder gebilligt.

From: Gewinnspiel NAW <gewinnspiel@netatwork.de>

To: Alex Wilber

Subject: Weihnachtstombola

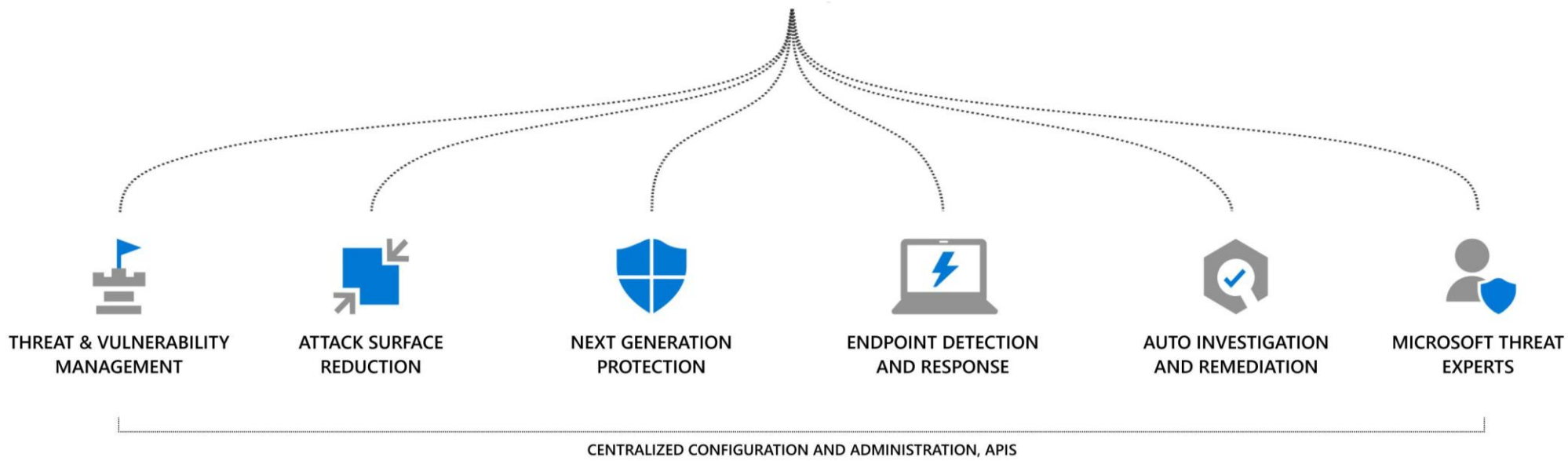
Attack Simulator - Auswertung



und wenn der Angreifer doch erfolgreich auf den Systemen ist....

Microsoft Defender

Identity **Office 365** **Cloud Apps** **Endpoint**

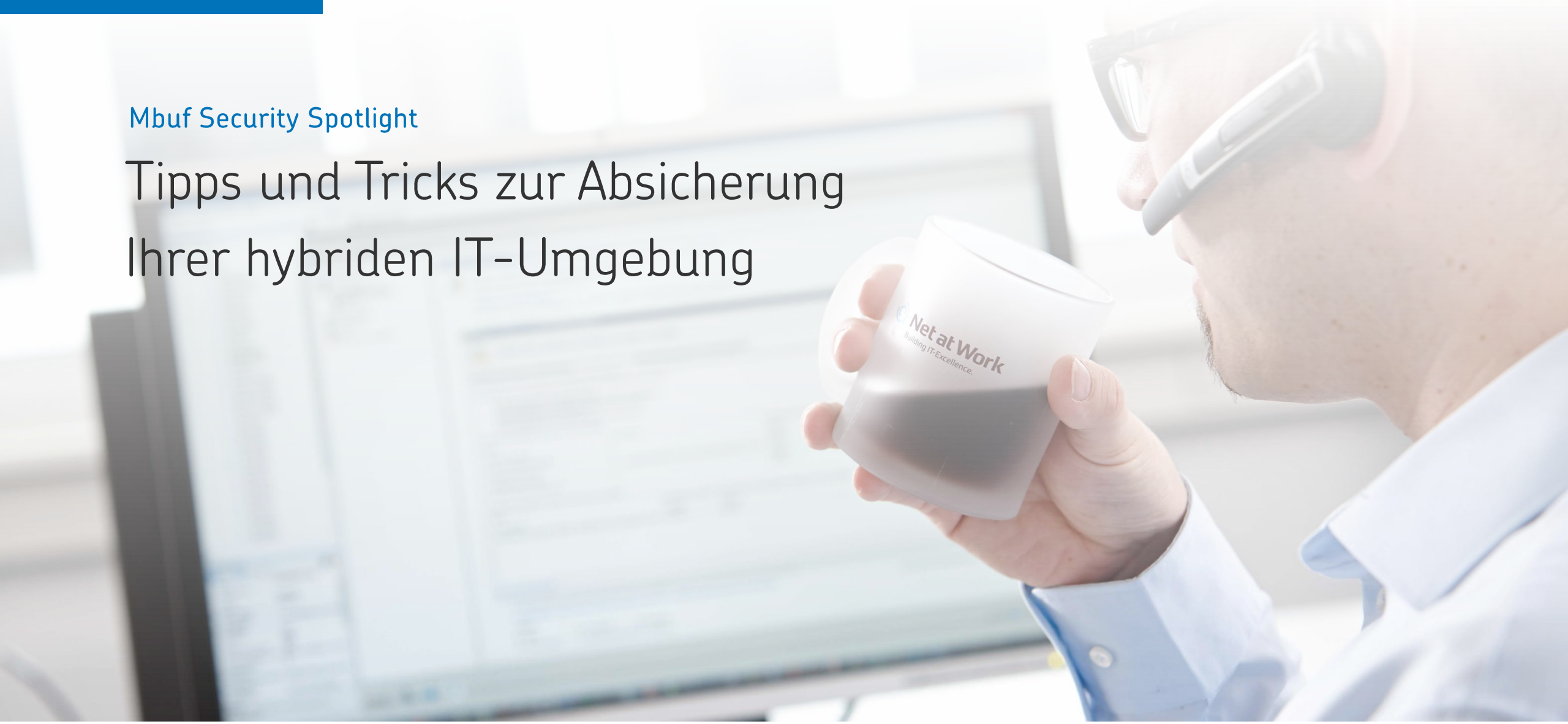


Was setzen wir zuerst um?

- Passwortpolicy überprüfen
- MFA und Regeln mit Conditional Access aufsetzen
- Nach und nach lokale Dienste über Azure AD App Proxy anbinden
- Geräteverwaltung einbinden -> Intune Device Compliance
- Härtung der Endgeräte
- Devices mit Defender for Endpoint schützen
- Patchmanagement
- Benutzersensibilisierung
- Domänencontroller mit Defender for Identity anbinden
- Schützen der administrativen Zugänge mit PIM
- Alte Protokolle deaktivieren
- Password Hash Sync aktivieren
- Security Alerts im SIEM sammeln
- E-Mail-Security mit SPF/DKIM/DMARC
- ....

Mbuf Security Spotlight

Tipps und Tricks zur Absicherung Ihrer hybriden IT-Umgebung



Net at Work
Building IT-Excellence.