HISCOX

Fake Tickets, echte Schäden: Cyberrisiken im WM -ype

Ihre Experten

Klemens Lemke

Underwriting Manager Cyber, Hiscox SA

Markus Drenger

Expert Digital Forensics & Incident Response @ HiSolutions

Die heutigen Themen

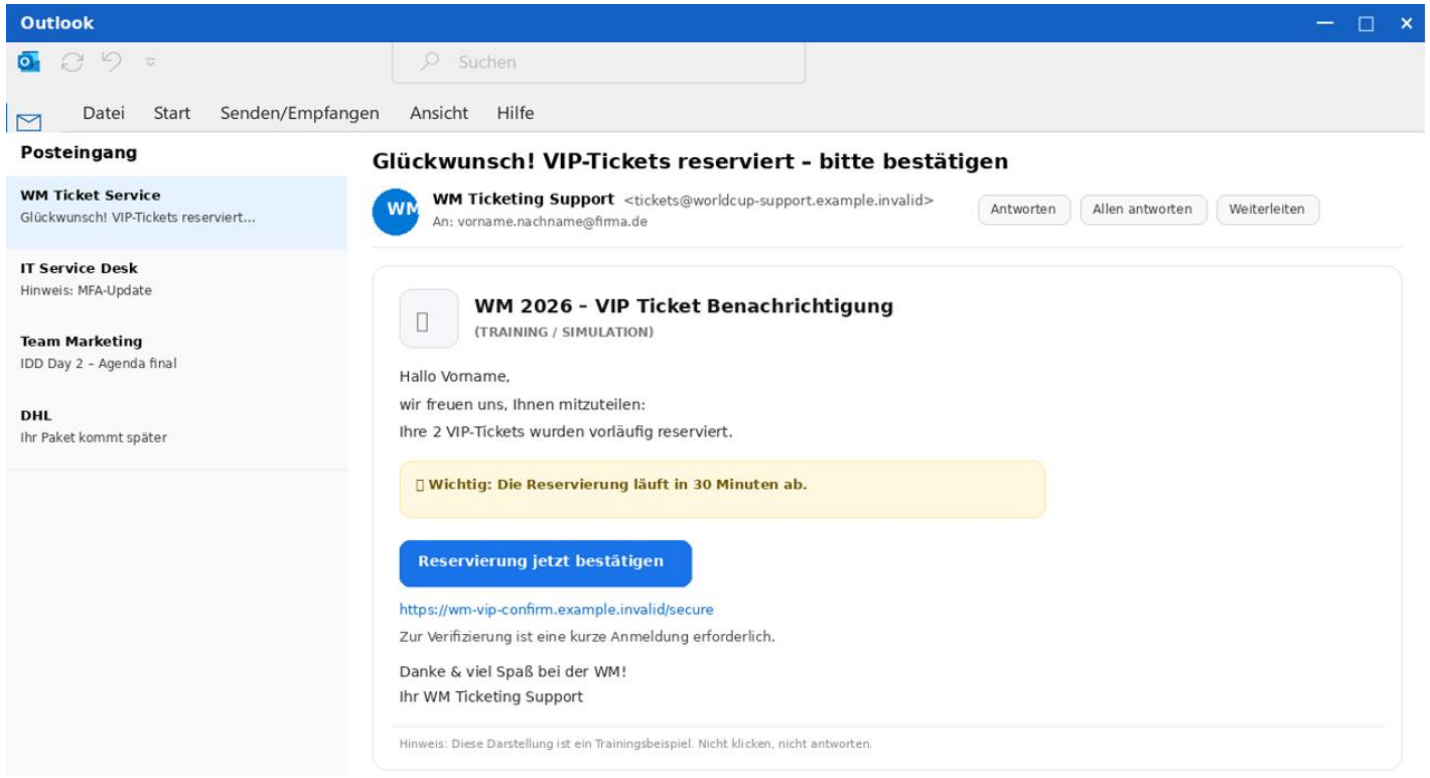
AGENDA

- Beispiele für gezieltes Phishing
- Einblicke in IT-Forensik und Wiederaufbau
- Was können wir alle tun, um uns zu schützen?

HISCOX

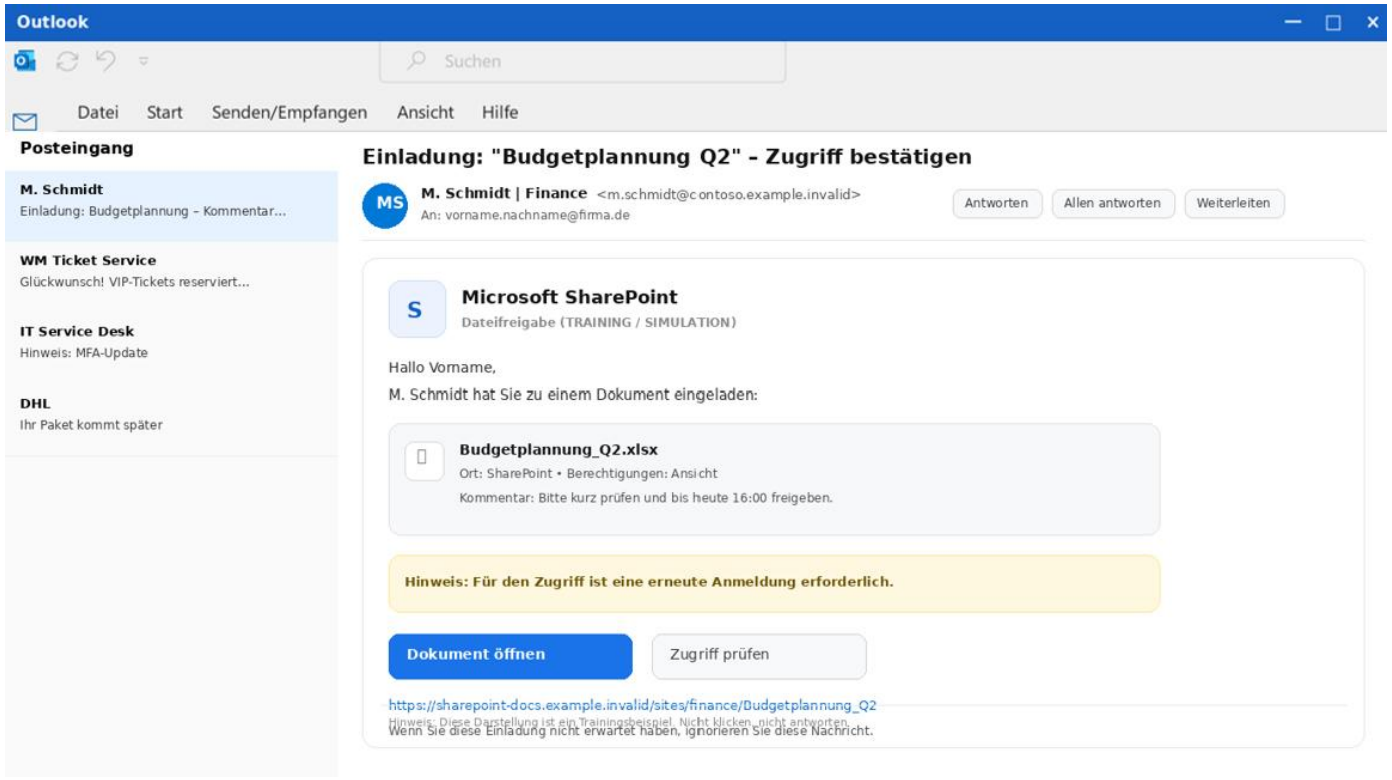
Beispiele für gezieltes Phishing

„Fataler Ticket-Klick“
Wie könnt so eine Phishing-Mail aussehen?



- **Köder:** Ticket-Mail mit Handlungsdruck
- **Klick** → Verschlüsslungstrojaner + Lösegeldforderung
- **Typische Kosten-/Schadenblöcke:** IT-Forensik & Krisenmaßnahmen, Wiederherstellung/Neuaufbau von Systemen &Daten sowie Betriebsunterbrechung und operative Notlösungen (z. B. Übergangsbetrieb)

„SharePoint-Einladung: Budgetplannung“
Wie könnt so eine Phishing-Mail aussehen?



- **Köder:** Interne SharePoint-Einladung mit scheinbar vertraulichen Dokumenten die es schnell zu prüfen gilt
- **Klick →** Weiterleitung auf die gefälschte Microsoft-Loginseite Erbeutung des Zugangsdaten
- **Typische Kosten-/Schadenblöcke:** IT-Forensik & Krisenmaßnahmen, Wiederherstellung/Neuaufbau von Systemen & Daten sowie Betriebsunterbrechung und Folgeschäden durch Missbrauch des Accounts

HISCOX

Einblicke in IT-Forensik und Wiederaufbau

HISOLUTIONS

HISCOX

Klick.

Wir schützen,
was Sie schätzen.

HISCOX

Phishing completed

Wir schützen,
was Sie schätzen.

HISCOX

Und jetzt?

Wir schützen,
was Sie schätzen.

HISCOX

Wie wird die Person in ihrem Unternehmen reagieren?

Wir schützen,
was Sie schätzen.

HISCOX

Ist das peinlich?

Wir schützen,
was Sie schätzen.

HISCOX

Wird ein Sicherheitsproblem erkannt?

Wir schützen,
was Sie schätzen.

HISCOX

Sind die Meldewege bekannt?

Wir schützen,
was Sie schätzen.

HISCOX

Wann wird auf die Meldung reagiert?

Wir schützen,
was Sie schätzen.

HISCOX

Die IT reagiert.

Wir schützen,
was Sie schätzen.

HISCOX

Passwort wird geändert.

Wir schützen,
was Sie schätzen.

HISCOX

Konto wird gesperrt.

Wir schützen,
was Sie schätzen.

HISCOX

Problem gelöst?

Wir schützen,
was Sie schätzen.

HISCOX

Betrifft die Kontosperrung alle Systeme?

Wir schützen,
was Sie schätzen.

HISCOX

Wurde das Passwort auch woanders verwendet?

Wir schützen,
was Sie schätzen.

HISCOX

Hat sich jemand nach dem Phishing eingeloggt?

Wir schützen,
was Sie schätzen.

HISCOX

Bei welchen Systemen war ein Login (ohne MFA) möglich?

Wir schützen,
was Sie schätzen.

HISCOX

Mobile Email?
VPN?
Citrix?
Website
Kunden- oder Lieferantenportal?

Wir schützen,
was Sie schätzen.

HISCOX

Was wird wo protokolliert?

Wir schützen,
was Sie schätzen.

HISCOX

Werden fehlgeschlagene Logins protokolliert?
Werden erfolgreiche Logins protokolliert?

Wir schützen,
was Sie schätzen.

HISCOX

Info aus der IT:
Es hat ein Login stattgefunden.

Wir wissen nicht, was gemacht wurde.

Wir schützen,
was Sie schätzen.

HISCOX

Gibt es einen IT-Sicherheitsvorfallsprozess?

Gibt es ein Playbook für IT-Sicherheitsvorfälle?

Wir schützen,
was Sie schätzen.

HISCOX

Was rät die IT?
Was empfiehlt ein IT-Dienstleister?

Wir schützen,
was Sie schätzen.

HISCOX

Passwort ändern und weitermachen?

Vorfall untersuchen lassen?

Wir schützen,
was Sie schätzen.

HISCOX

Ist ausreichendes IT-Forensik-Knowhow intern vorhanden?

Wir schützen,
was Sie schätzen.

HISCOX

Was, wenn eine Hintertür installiert wurde?

Wir schützen,
was Sie schätzen.

HISCOX

Wenn neue Email-Filterregeln eingehende Emails weiterleiten?

Wir schützen,
was Sie schätzen.

HISCOX

Auf welche Systeme wurde zugegriffen?
Was wurde verändert?
Besteht ein Risiko für die IT-Umgebung?

Wir schützen,
was Sie schätzen.

HISCOX

Wurde auf Daten zugegriffen? Kam es zu einer meldepflichtigen Datenschutzverletzung?

Wir schützen,
was Sie schätzen.

HISCOX

Sind von dort aus weitere IT-Systeme angegriffen worden?

Waren die Angriffe erfolgreich?

Wir schützen,
was Sie schätzen.

HISCOX

Ist die Tür erst einmal offen, bieten sog. Access Broker Zugangsdaten zum Kauf an.

Wir schützen,
was Sie schätzen.

HISCOX

Was hilft?

Wir schützen,
was Sie schätzen.

Was können wir alle tun, um uns zu schützen?

Tipps:
Was kann ich tun um meine Cyber Resilienz zu erhöhen?

- ✓ MFA kosequent: Phishing-Zugänge bleiben wirkungslos, auch bei gestohlenen Passwörtern
- ✓ Externe E-Mails klar kennzeichnen: Gefälschte Absender schneller erkennen
- ✓ 4-Augen-Prinzip verpflichtend bei Zahlungen, Datenänderungen und ungewöhnlichen Anfragen
- ✓ Verifikation über abweichenden Kommunikationsweg: Telefon oder Rücksprache im Haus, sofern von intern
- ✓ Belegschaft regelmäßig trainieren: Schulungen, Phishing-Tests, etc.
- ✓ IT-Security auf aktuellen Stand halten: Patches und Updates einspielen, Altsysteme vermeiden

Wie die Cyberversicherung unterstützt…
Cyber by Hiscox

HISCOX

	Vor dem Angriff		Während des Angriffs		Nach dem Angriff	
Das leistet CyberClear by Hiscox	Cyber-Training & Phishings-Test	Risikominimierung	Krisenplan	Roter Faden im Ernstfall	Haftpflicht	Abwehr & Erfüllung, inkl. Medienhaftpflicht …
	Cyber-Sicherheits-Scan	Schwachstellenanalyse	Soforthilfe 24/7 HISOLUTIONS .msg	Führende IT-Forensiker und Experten für die Schadenanalyse und die Systemwiederherstellung	Eigenschäden	**Nur bei Hiscox:** Forderungsausfall-deckung bei manipu-lierten Zahlungsdaten …
	Norton-Schutzpaket[1] norton	Umfassender Schutz für Geräte und Daten	Experten-netzwerk	Fachanwälte & PR-Krisenberater	Betriebsunter-brechung	**Nur bei Hiscox:** Tagessatzentschädigung für schnelle Leistung ohne komplizierten Nach-weis des Ertragsausfalls …

1) Optional abschließbar mit CyberClear Plus

HISCOX

Vielen Dank für Ihre Aufmerksamkeit