MYNI GMEIND

in Partnerschaft mit

Schweizerischer Gemeindeverband
Association des Communes Suisses
Associazione dei Comuni Svizzeri
Associaziun da las Vischnancas Svizras

Die “menschliche Firewall” stärken

Stefan Haller | Managing Partner
stefan.haller@linkyard.ch

linkyard

Stefan Haller

Eidg. Dipl. Ing. Informatik FH, EMBA General Management, CAS Cyber Investigation & Digital Forensics

FH-Dozent für Informationssicherheit und Projektmanagement

20 Jahre Projekterfahrung im öffentlichen Sektor

Berater und Auditor für Sicherheits-Management-Systeme

Wer greift uns an?

Wie Menschen versagen

Fazit

Wer greift uns an?

Wer greift uns an?

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer




DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

CAUTION

Maksim Viktorovich Yakubets is wanted for his involvement with computer malware that infected tens of thousands of computers in both North America and Europe, resulting in actual financial losses in the tens of millions of dollars.

Specifically, Yakubets was involved in the installation of malicious software known as Zeus, which was disseminated

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

aud; Bank Fraud;
r

ne

ly 170 pounds

Rewards Program is offering a
nviction of Maksim Viktorovich

re that infected tens of thousands of computers in both North America and Europe, resulting in actual financial losses in the tens of millions of dollars. Specifically, Yakubets was involved in the installation of malicious software known as Zeus, which was disseminated

Kapitalismus in Aktion
–
von neugierigen Nerds zu professionellen Unternehmern

Wer greift uns an?

Wie Menschen versagen

Fazit

„Menschen sind oft das schwächste Glied in der Sicherheitskette und chronisch für das Versagen von Sicherheitssystemen verantwortlich.“

-- Bruce Schneier, ”Secrets and Lies”, 2000, p. 149

Menschen **tun Dinge**
die sie nicht hätten machen sollen

Umgangssprachlich:
“eine Dummheit begehen”

Menschen **machen Dinge nicht**
die sie hätten tun sollen

Umgangssprachlich:
“etwas versäumen”

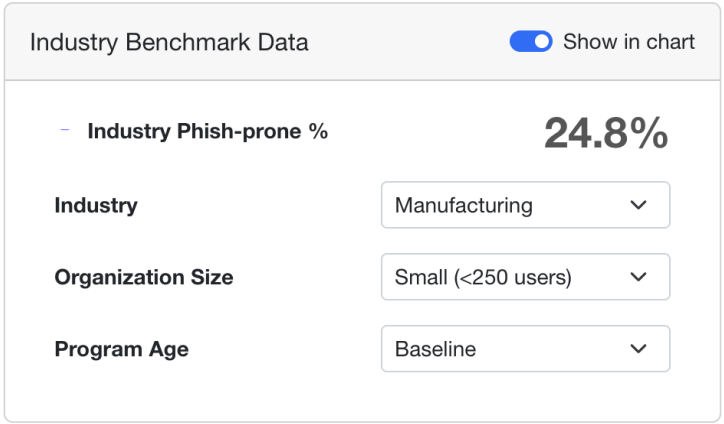
Statistiken zur Bedrohungslage

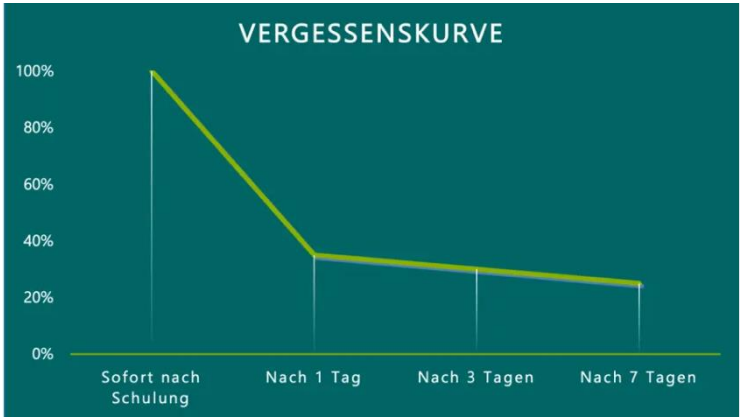
Gemäss Bundesamt für Cybersicherheit (BACS) sind seit der Einführung der Meldepflicht im letzten Frühling 28 Meldungen von Gemeinden eingegangen. Die häufigsten Themen sind:

- Phishing / Social-Engineering
- Business-E-Mail-Compromise (BEC)
- CEO-Fraud
- Malware / Ransomware

Dauerbrenner

Phishing bleibt erfolgreich



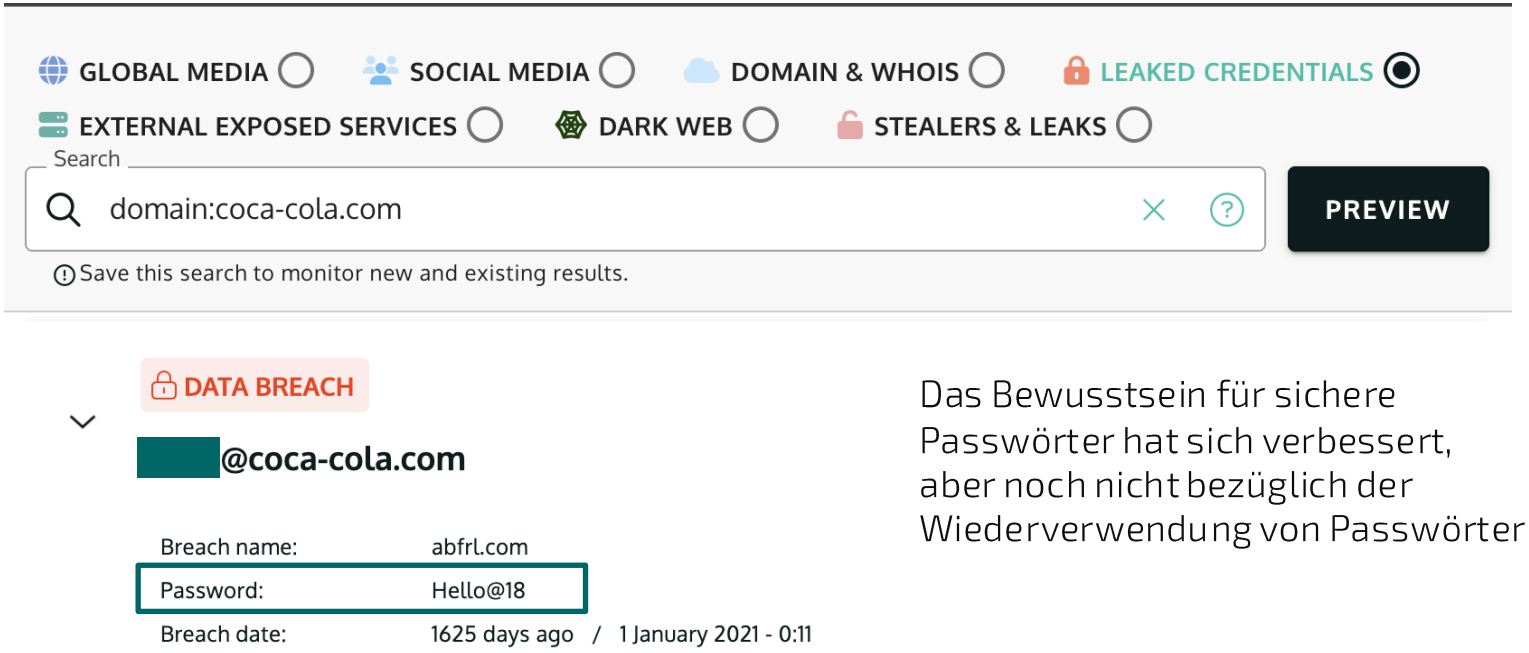


Phishing führt nach wie vor zum Erfolg, E-Mails sind weiterhin der wichtigste Kanal für Betrugsversuche und Ransomware.

Selbst bei regelmäßigem Training ist es nur eine Frage der Zeit, bis jemand hereinfällt.
...und ohne regelmässiges Training kann man es auch schneller haben.

Dauerbrenner

Schwache & wiederverwendete Passwörter



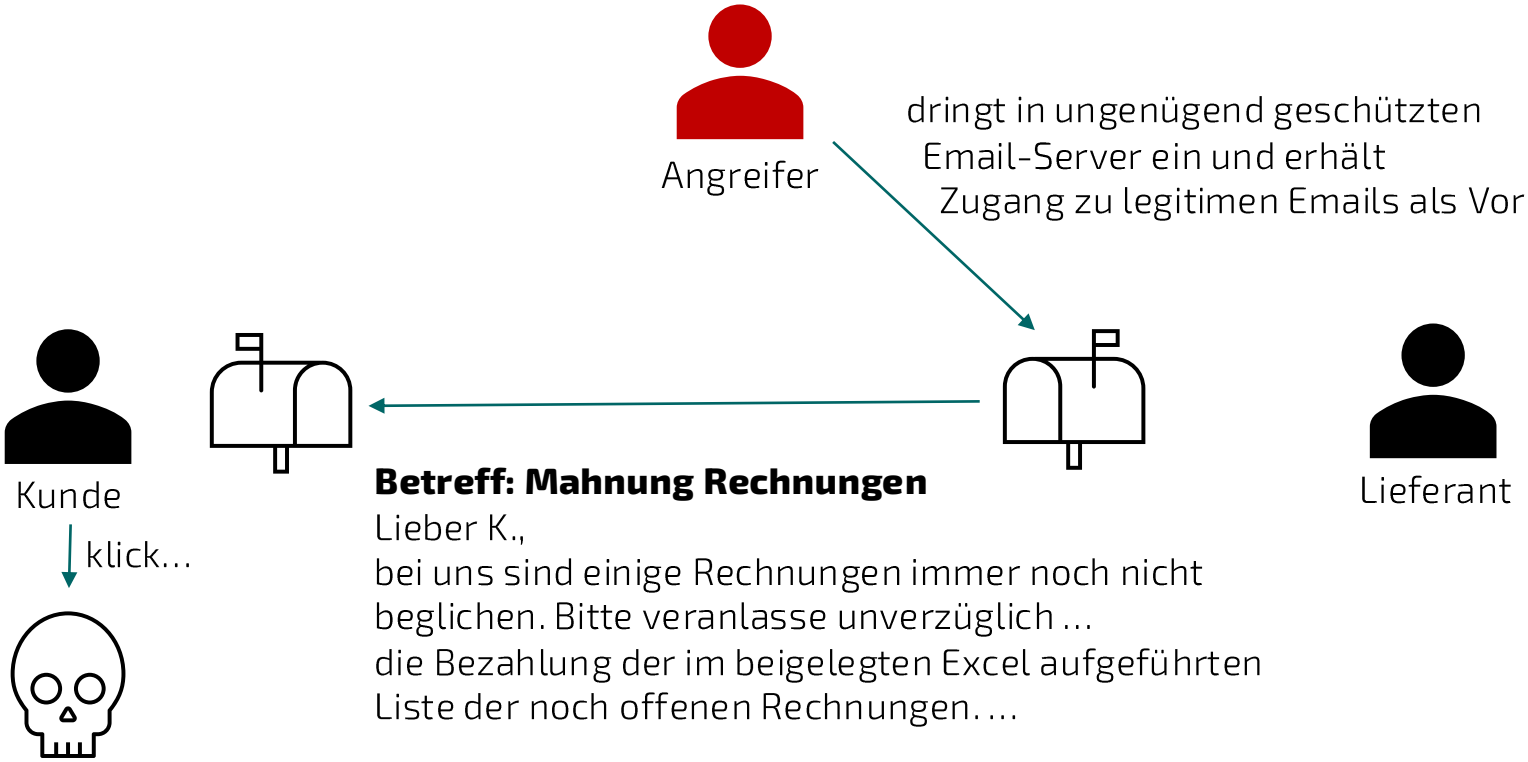
Das Bewusstsein für sichere Passwörter hat sich verbessert, aber noch nicht bezüglich der Wiederverwendung von Passwörtern.

Passwort-Manager verwenden, Zweifaktorauthentifizierung nutzen wo immer möglich

Dank künstlicher Intelligenz ist es jetzt viel einfacher, Betrug zu begehen.

Praxisfall

Anonymisiertes Fallbeispiel: Business E-Mail Compromise



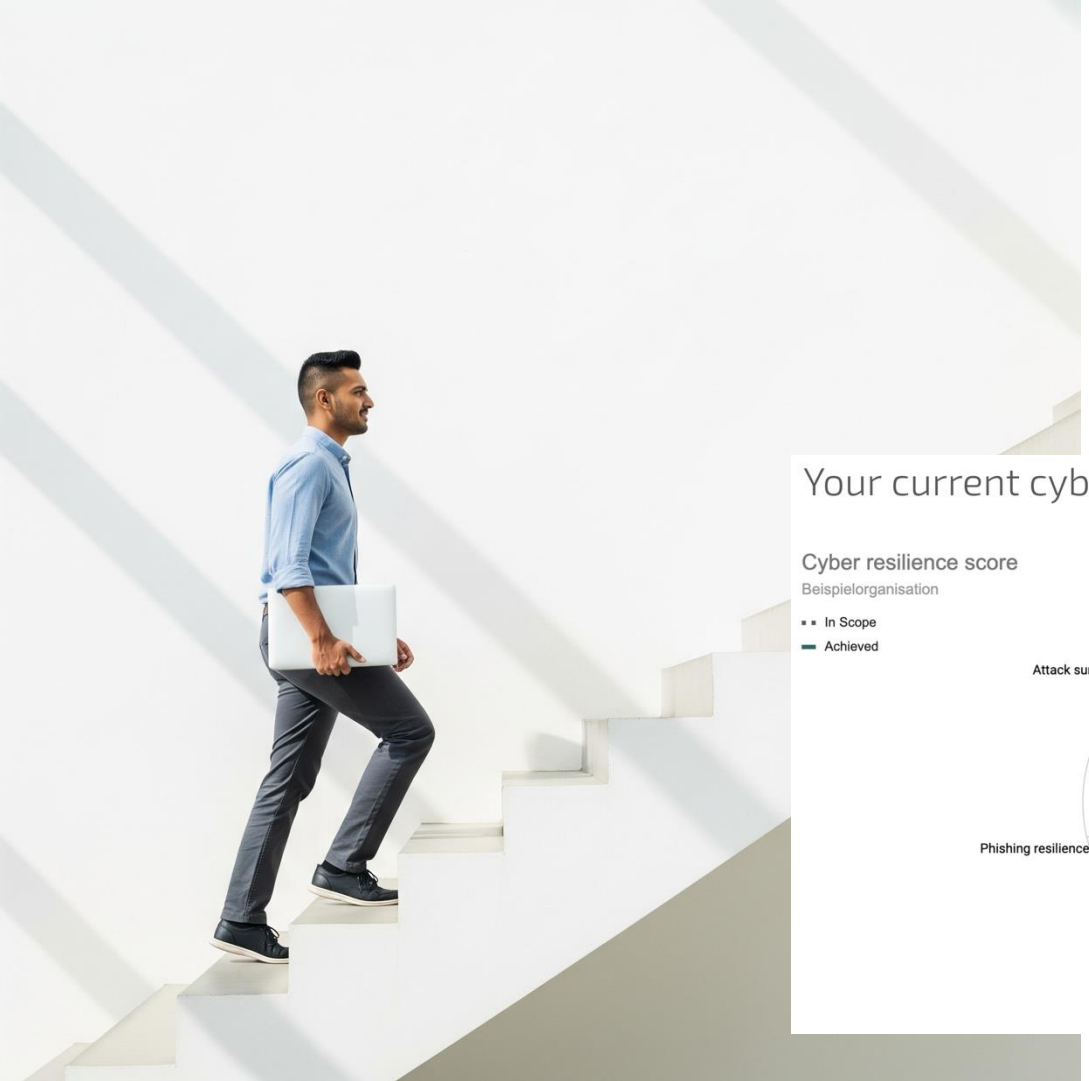
Wer greift uns an?

Wie Menschen versagen

Fazit

Fazit: Checkliste

- [ ] Technik professionell überwachen und beaufsichtigen, aber auch …Mitarbeitende regelmässig sensibilisieren.
- [ ] Mitarbeitende regelmässig sensibilisieren, aber auch …Notfallplan vorbereiten.
- [ ] **Für heikle Aufgaben: Sichere Protokolle definieren und befolgen**
- [ ] **Kontinuierliche Prüfung der Risiken und Verbesserung der Massnahmen**



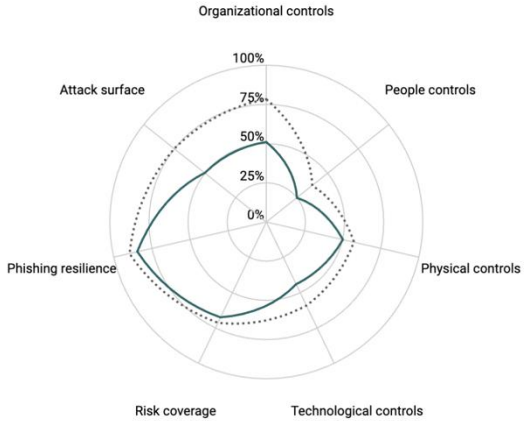
Wissen, wo man steht und sich kontinuierlich verbessern

Your current cyber resilience score

Cyber resilience score

Beispielorganisation

- In Scope
- Achieved



Overall score: 53%

Scope coverage: 67%

In-scope score: 79%

as of 22.11.2024

Stefan Haller

Managing Partner

stefan.haller@linkyard.ch
+41 78 746 5116
Termin: https://calendly.com/stefan-linkyard

linkyard ag