31.03.2026

Cyberbedrohungslage: Phishing weiterhin grösste Gefahr für Unternehmen und Privatpersonen

Der aktuelle Halbjahresbericht des Bundesamts für Cybersicherheit (BACS) zeigt: Die Cyberbedrohungslage in der Schweiz bleibt auf konstant hohem Niveau. Besonders im Fokus stehen weiterhin Betrugsdelikte – allen voran Phishing.

Phishing: Vom Massenangriff zur gezielten Täuschung

Phishing gehört nach wie vor zu den häufigsten und gleichzeitig effektivsten Angriffsmethoden. Cyberkriminelle nutzen täuschend echte E-Mails, SMS oder Webseiten, um an vertrauliche Daten wie Zugangsdaten oder Kreditkarteninformationen zu gelangen.

Während klassische Massen-Phishing-Kampagnen weiterhin verbreitet sind, zeigt sich eine klare Entwicklung hin zu deutlich raffinierteren Methoden:

- **Zielgerichtetes Spear-Phishing**: Angriffe werden individuell auf Personen oder Organisationen zugeschnitten.
- **Real-Time-Phishing**: Opfer werden während des Login-Prozesses aktiv manipuliert.
- **Voice-Phishing (Vishing)**: Betrüger geben sich telefonisch als Bank oder Behörde aus.

Gerade diese Kombinationen erhöhen die Erfolgsquote erheblich, da sie Vertrauen schaffen und bestehende Sicherheitsmechanismen umgehen.

Neue Phishing-Methoden in der Schweiz

Besonders auffällig ist die zunehmende Anpassung der Angriffe an Schweizer Gegebenheiten. So nutzen Täter gezielt bekannte Marken, Treueprogramme oder Dienstleistungen, um ihre Angriffe glaubwürdiger zu gestalten.

Erstmals wurden in der Schweiz sogenannter **SMS-Blaster** eingesetzt. Dabei senden Angreifer Phishing-Nachrichten direkt über gefälschte Mobilfunkantennen an Smartphones in der Umgebung und umgehen so klassische Schutzmechanismen der Netzbetreiber.

Ziel: Mehr als nur Zugangsdaten

Moderne Phishing-Angriffe zielen längst nicht mehr nur auf Passwörter. Immer häufiger versuchen Angreifer, umfassende Datenprofile zu erstellen. Dazu gehören unter anderem:

- Persönliche Angaben
- Finanzinformationen
- Telefonnummern

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

Diese Daten werden für weiterführende Angriffe, Identitätsdiebstahl oder den Verkauf im Darknet genutzt.

Unternehmen besonders im Visier

Auch Unternehmen sind stark betroffen. Neben klassischen Phishing-Angriffen treten vermehrt folgende Varianten auf, die teilweise zu erheblichen finanziellen Schäden führen können:

- CEO-Betrug (https://www.ebas.ch/ceo-fraud/)
- Rechnungsmanipulation (https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden/aktuelle-bedrohungen/bec-betrug.html)
- Kombinierte Social-Engineering-Angriffe (https://www.ebas.ch/social-engineering/)

Handlungsempfehlungen

Angesichts der zunehmenden Professionalität der Angreifer sind technische und organisatorische Massnahmen entscheidend:

- Öffnen Sie keine Links aus unbekannten Nachrichten.
- Geben Sie sensible Daten niemals über verlinkte Webseiten ein.
- Aktivieren Sie die Multi-Faktor-Authentisierung (MFA).
- Prüfen Sie Absender und Anfragen kritisch.
- Melden Sie verdächtige Vorfälle.

Besonders wichtig: **Phishing lebt von Zeitdruck und Emotionen. Wer sich einen Moment Zeit nimmt und Anfragen hinterfragt, kann viele Angriffe bereits im Keim ersticken.**

Fazit

Phishing bleibt die zentrale Cyberbedrohung in der Schweiz und entwickelt sich kontinuierlich weiter. Die zunehmende Kombination verschiedener Angriffsmethoden sowie die stärkere Personalisierung machen es für Nutzerinnen und Nutzer immer schwieriger, Betrugsversuche zu erkennen.

Umso wichtiger sind Sensibilisierung, klare Prozesse und ein bewusster Umgang mit digitalen Informationen – sowohl im privaten als auch im geschäftlichen Umfeld.

Halbjahresbericht 2025/2 des BACS (https://cms.news.admin.ch/dam/de/bacs/cFWQRo2eonAz/BACS-HJB-2025-2_DE.pdf)

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik