

CSBW-Factsheet: Cybersecurity-Wissen kompakt

CYBERANGRIFFE IM KONTEXT BEWAFFNETER KONFLIKTE

In bewaffneten Konflikten des 21. Jahrhunderts wie dem Krieg in der Ukraine finden parallel zu den Auseinandersetzungen vor Ort Angriffe im Cyberraum statt, die durch die globale Vernetzung unserer IT-Systeme über viele Grenzen hinweg gehen.

Auch wenn der Ort des Konflikts weit weg erscheint, kann ein Angriff im Cyberraum auch **Ihren Rechner** erreichen.

Ausgangslage:

- › Kriegerische Auseinandersetzungen und andere bewaffnete Konflikte werden zunehmend durch Cyberattacken begleitet.
- › Sowohl staatliche als auch nicht-staatliche Gruppen aller Seiten können hier die aktive Rolle in einem Angriff einnehmen.
- › Ziel der Angriffe ist es, die Systeme der anderen Seite zu infiltrieren, deren IT-Infrastruktur zu stören oder außer Betrieb zu setzen, mit Auswirkungen bis in die KRITIS-Bereiche¹ hinein.
- › Auch scheinbar Unbeteiligte können Ziele oder Zwischenziele der Cyberangriffe sein.
- › Die Konflikte werden im Cyberraum fast immer von Desinformation² begleitet, insbesondere über soziale Netzwerke.
- › Phishing-Mails³ sind nach wie vor ein häufiges Einfallstor. Prüfen Sie Links in E-Mails und E-Mail-Anhänge genau, bevor Sie sie öffnen!

Handlungsempfehlungen in Zeiten der Konflikte:

- › Seien Sie besonders aufmerksam und sensibilisieren Sie auch andere in Ihrem Umfeld zu erhöhter Aufmerksamkeit.
- › Behalten Sie aktuelle Entwicklungen im Cyberraum im Blick und nutzen Sie dabei seriöse Quellen und Nachrichtenkanäle.
- › Nutzen Sie zur Verwaltung von Passwörtern einen Passwortmanager.
- › Wenn technische Schutz-Vorkehrungen verschärft werden müssen, haben Sie bitte dafür Verständnis. Das geht oft zwar zu Lasten des Komforts, z. B. bei strengeren Spam-Filtern oder einer Zwei-Faktor-Authentifizierung, erhöht aber die Sicherheit erheblich.
- › Seien Sie auf den Notfall vorbereitet: Wissen Sie, wie Sie im Cybernotfall richtig reagieren? Was machen Sie bei Verdacht auf eine Phishing-Mail? Wie reagieren Sie bei einem Komplettausfall Ihrer IT-Systeme?

¹ „Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ Quelle: bsi.bund.de

² „Irreführende und falsche Informationen werden [...] zu einer Gefahr, wenn sie das Ziel haben, Menschen vorsätzlich zu täuschen oder zu beeinflussen und gezielt verbreitet werden. Man spricht dann von **Desinformation**.“
Quelle: bundesregierung.de

³ **Phishing-Mails** sind E-Mails, über die mit Betrugsabsicht versucht wird, von Ihnen Daten zu erlangen oder Schadsoftware auf Ihrem Rechner auszuführen.

Sehr geehrter Sparkassen-Kunde,

Durch das aktuelle Vorgehen der russischen Regierung und den damit einhergehenden Sanktionen der Europäischen Union, sind alle Banken in der EU dazu verpflichtet sicherzustellen, dass alle ihre Kunden sich an die neuen Sanktionen halten.

Deswegen ist eine erneute Verifikation ihrer Daten notwendig.

Bei ausbleibender Identifikation bis zum 14.03.2022, sind wir nach EU Recht dazu verpflichtet, Ihr Konto zu schließen und Ihr Guthaben einzufrieren.

Nach erfolgreicher Verifizierung wird sich ein Kundenberater mit Ihnen in Verbindung setzen, um den Vorgang abzuschließen.

Weiter zur Website

Mit freundlichen Grüßen
Ihr Service Team

Beispiel einer echten Phishing-Mail

Quelle: https://twitter.com/bsi_bund/status/1503308780582416386