

## **Barrierefreie Version**

### **CSBW-Factsheet: Cybersecurity-Wissen kompakt**

#### **Zum Thema: CYBERANGRIFFE IM KONTEXT BEWAFFNETER KONFLIKTE**

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

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

#### **Ausgangslage:**

Kriegerische Auseinandersetzungen und andere bewaffnete Konflikte werden zunehmend durch Cyberattacken begleitet.

Sowohl staatliche als auch nichtstaatliche Gruppen aller Seiten können hier die aktive Rolle eines Angreifers annehmen.

Ziel der Angreifer 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-Bereiche<sup>1</sup> hinein.

Auch scheinbar Unbeteiligte können Ziele oder Zwischenziele der Cyberangriffe sein.

Die Konflikte werden im Cyberraum fast immer von Desinformation<sup>2</sup> begleitet, insbesondere über Soziale Medien.

Phishing-Mails<sup>3</sup> 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 wie z. B. KeePass.

Wenn technische Schutzvorkehrungen verschärft werden müssen, haben Sie bitte dafür Verständnis. Das geht oft zwar zu Lasten des Komforts, z. B. bei strengeren

Spamfiltern oder einer Zwei-Faktor-Authentifizierung, aber erhöht die Sicherheit teils erheblich.

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? Eine gute Vorbereitung auf den Notfall kann weitreichende Schäden verhindern.

### Beispiel einer echten Phishing-Mail im Kontext des Ukraine-Kriegs

Mit Bezug zu den Russland-Sanktionen sind nun auch betrügerische E-Mails im Namen von Banken im Umlauf. Die Kriminellen geben bspw. vor, dass man kontrollieren müsse, ob sich die Kundinnen und Kunden an Sanktionen halten. Dabei handelt es sich in jedem Fall um Phishing-Versuche!

Quelle: [BSI auf X: „Mit Bezug zu den Russland-Sanktionen sind nun auch betrügerische E-Mails im Namen von Banken im Umlauf. Die Kriminellen geben bspw. vor, dass man kontrollieren müsse, ob sich die Kundinnen und Kunden an Sanktionen halten. Dabei handelt es sich in jedem Fall um #Phishing-Versuche! https://t.co/vHbv7U6vjE“ / X \(twitter.com\)](https://t.co/vHbv7U6vjE)

Folgende Abbildung zeigt eine E-Mail einer vermeintlichen Sparkasse.



Abbildung 1: E-Mail der vermeintlichen Sparkasse. Text im Folgenden.

Text der abgebildeten E-Mail der vermeintlichen Sparkasse:

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.

Button: Weiter zur Webseite

Mit freundlichen Grüßen

Ihr Service Team

*(Ende des Textes der E-Mail)*

### **Quellen:**

<sup>1</sup> „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](https://www.bsi.bund.de)

<sup>2</sup> „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](https://www.bundesregierung.de)

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

Weitere Factsheets und Informationen unter: [www.cybersicherheit-bw.de](https://www.cybersicherheit-bw.de)

CSBW – Abteilung 1: Prävention – Stand 05.2023

Kontakt: [schulungen@cybersicherheit.bwl.de](mailto:schulungen@cybersicherheit.bwl.de)