

## Cyberregeln für mehr Sicherheit – zu Hause, im Dienst und bei der Arbeit

### REGEL 1: ZURÜCKHALTUNG BEI SOCIAL MEDIA

Bereits anhand ein paar weniger Beiträge aus den sozialen Medien kann eine Vielzahl an Informationen zusammengetragen werden. Äusserungen und Beiträge in sozialen Medien sind daher immer als öffentlich zu betrachten und sollten dem Grundsatz «weniger ist mehr» folgen.

### REGEL 2: VORSICHT VOR USB-GERÄTEN

Angreifer können mittels USB-Sticks oder manipulierter USB-Kabel auf das System der Zielperson und deren Daten, Kameras, Mikrofone und Tastaturen zugreifen. Es dürfen auf keinen Fall USB-Geräte, deren Herkunft unklar ist, benutzt werden. Private Geräte dürfen am Arbeitsplatz nicht verwendet werden und umgekehrt.

### REGEL 3: ÖFFENTLICHE HOTSPOTS SIND ZU MEIDEN

Sämtliche Zugangsdaten, welche über manipulierte, öffentliche Drahtlosnetzwerke eingegeben werden, können abgefangen werden. Öffentlich zugängliche Hotspots werden oft zur Verbreitung von Viren und zum Datenklau benutzt. Die Verwendung eines persönlichen Hotspots via Mobilfunknetz bietet unterwegs eine deutlich sicherere Alternative.

### REGEL 4: WLAN, BLUETOOTH, GPS GENERELL AUSSCHALTEN

Bereits mit geringem Aufwand können sich Angreifer Zugang zu Mobiltelefonen oder Laptops verschaffen und diese als Sensoren einsetzen. Dienste wie WLAN, NFC, Bluetooth und Ortungsdienste sind generell ausgeschaltet und sollen nur bei unmittelbarem Gebrauch aktiviert werden.

### REGEL 5: MÖGLICHERWEISE SIND GERÄTE BEREITS INFIZIERT

Aufgrund der verdeckten Natur von Cyber-Angriffen lässt sich die Kompromittierung eines Geräts nie zu 100% ausschliessen. Um zu verhindern, dass klassifizierte Informationen abfliessen, dürfen Geräte wie Laptops, Tablets, Smartphones und -watches keinesfalls im selben Raum sein, wenn vertrauliche oder geheime Gespräche stattfinden.

### REGEL 6: UNBEKANNTE ABSENDER SIND VERDÄCHTIG

Links, QR-Codes und Anhänge sind häufig genutzte Angriffsvektoren. Im Zweifelsfall sollte die Legitimität der Nachricht durch eine telefonische Nachfrage beim Absender geklärt werden.

### REGEL 7: VORFÄLLE IMMER MELDEN

Beim geringsten Verdacht auf eine Virusinfektion ist die Netzwerkverbindung schnellstmöglich zu trennen. Das Gerät sollte jedoch zwecks Spurensicherung nicht ausgeschaltet werden. Im beruflichen Umfeld ist unverzüglich die Meldung via Helpdesk oder IT-Verantwortlicher zu erstatten, und im Privaten ist die Polizei die richtige Anlaufstelle für Cyberkriminalität.

### REGEL 8: STARKE PASSWÖRTER SCHÜTZEN!

Nach Möglichkeit ist die sogenannte Zwei-Faktor-Authentifizierung, bestehend aus Einmal-Passwort mit mindestens 12 Zeichen, Klein- und Grossbuchstaben, Zahlen und Sonderzeichen, sowie einem SMS-Token, zu aktivieren. Dadurch kann auf eine zyklische Passwortänderung verzichtet werden.

### Veranstaltungskalender 2024

Datum	Veranstaltung 2024	Ort	Organisation
7. November 2024	Chance Miliz	AAL Luzern	KOG Luzern
22. November 2024	168. GV der OG Uri	SBU Schattdorf	OG Uri

# BULLETIN OG URI



Altdorf anno 1850

# Cyber-Security

**Phishing-Attacken, Verschlüsselungstrojaner oder Datenklau: Das sind Beispiele jener Bedrohungen, die ständig im Cyber-Raum lauern. Auch die Schweiz und ihre Bürgerinnen und Bürger werden nicht von Cyber-Angriffen verschont. Nebst der persönlichen Eigenverantwortung eines jeden Nutzers von Informations- und Kommunikationstechnologien (IKT) im privaten, dienstlichen und beruflichen Umfeld obliegt der Schutz der Schweiz und ihrer Bevölkerung im Wirkungsraum Cyber- und elektromagnetischer Raum (CER) der Schweizer Armee. Die Spezialisten des Kommando Cyber (Kdo Cy) sind dabei verantwortlich für den Schutz und die Weiterentwicklung der einsatzkritischen IKT-Infrastruktur der Schweizer Armee, stellen den Wissens- und Entscheidvorsprung über alle Lagen und in allen Wirkungsräumen sicher und nehmen durch Aktionen im CER gezielt Einfluss auf die Einsätze der Schweizer Armee und konzentrieren sich dabei vollständig auf die einsatzkritischen Leistungen der Armee und ihrer Partner.**

Es freut den Vorstand der OG Uri daher ausserordentlich, am 22. November 2024 den Chef Kommando Cyber, Herrn Divisionär Simon Müller, anlässlich der 168. GV in seinen Reihen begrüssen zu dürfen.

Folgender Text soll einen Überblick über die aktuellen Bedrohungen, Akteure und Angriffsformen, mit welchen im Cyber-Raum gerechnet werden muss, bieten sowie einige Regeln zur sofortigen Erhöhung der individuellen Cyber-Sicherheit im Privaten, im Dienst oder am Arbeitsplatz aufzeigen.

## Cyber-Bedrohung, -Akteure und -Angriffsformen

Die Bedrohungen durch Cyber-Angriffe sind in den letzten Jahren stark gestiegen. Erfolgreich durchgeführte Angriffe im In- und Ausland mit teilweise gravierenden Konsequenzen haben gezeigt, dass nicht nur die Häufigkeit und Komplexität der Cyber-Angriffe zunehmen, sondern diese auch vermehrt zielgerichtet gegen Staaten oder Unternehmen eingesetzt werden. Zur Einschätzung der Lage ist es angesichts der Vielzahl von möglichen Cyber-Angriffen wichtig, zwischen verschiedenen Phänomenen zu unterscheiden. Unterscheidungskriterien sind der Zweck der Angriffe, die Akteure, welche hinter den Angriffen stehen, und der Kreis jener, welche angegriffen werden. Auf dieser Grundlage lassen sich fünf verschiedene Cyber-Bedrohungen und -Akteure sowie fünf verschiedene Formen der Cyber-Angriffe unterscheiden (s. Darstellung), wobei zu beachten ist, dass diese häufig in Kombination auftreten und zwischen ihnen Überschneidungen bestehen.

### BEDROHUNG UND -AKTEURE

Cyber-Akteure	Cyber-Mächte				
	Gezielte und unerkennbare Bedrohungsagenten				
	Professionelle Organisationen, Cyber-Kriminelle				
	Entwickler von Verwundbarkeiten, motivierte Hacker				
	Anwender von Hacking-Tools				
		Aktivismus	Kriminalität	Terrorismus	Konflikt
		Cyber-Bedrohung			

### ANGRIFFSFORMEN

**Cyber-Kriminalität** beschreibt Straftaten, welche mithilfe von IKT oder durch Nutzung von Schwachstellen dieser Technologien verübt werden. In der Regel steht das Motiv der Bereicherung im Vordergrund, da mit relativ geringem Aufwand hohe Gewinne möglich sind und das Risiko auf Strafverfolgung, insbesondere im internationalen Rahmen, gering ist. Unternehmen, Behörden und Bevölkerung sind dabei gleichermassen gefährdet, und die Eintrittswahrscheinlichkeit ist als sehr hoch zu bewerten. Für die ins Visier geratenen Individuen oder Organisationen korreliert dies oftmals mit einem hohen Schadenspotenzial.

**Cyber-Sabotage und -Terrorismus** ist das Stören oder Zerstören von IKT. Obwohl der Angriff im Cyber-Raum erfolgt, können die Folgen je nach Art der Sabotage physische Auswirkungen mit weitreichenden Konsequenzen verursachen. Beispiele hierfür sind das gezielte Angreifen von kritischer Infrastruktur im Energie- oder Transportbereich. In der Schweiz wurden bislang noch keine grösseren Fälle bekannt, sollte die Schweiz oder Organisationen mit Sitz in der Schweiz aber aus politischen Gründen zukünftig in den Fokus von staatlichen oder nicht staatlichen Akteuren mit den entsprechenden Fähigkeiten geraten, würde die Eintrittswahrscheinlichkeit schnell stark ansteigen und ein hohes Schadenspotenzial aufweisen.

**Desinformation und Propaganda** ist mittlerweile eine allgegenwärtige Bedrohung im Cyber-Raum und wird in vielen Ländern, insbesondere vor wichtigen Wahlen oder Abstimmungen, deutlich intensiviert. Auch in der Schweiz ist damit zu rechnen, dass staatliche- oder nichtstaatliche Akteure versuchen, das Vertrauen der Bürgerinnen und Bürger in den Staat und Institutionen zu unterminieren. Aufgrund der steigenden Bedrohung von sozialen Medien als Informationsquellen ist davon auszugehen, dass das mittlere Schadenspotential zukünftig mit der bereits jetzt sehr hohen Eintrittswahrscheinlichkeit weiter ansteigen wird.

**Cyber-Konfliktführung** aller Art wird in den aktuellen, hybrid-geführten Konflikten als Mittel der Kriegsführung flankierend zu den militärischen, politischen, wirtschaftlichen und kriminellen Mitteln eingesetzt. Dabei werden Verantwortlichkeiten bewusst verschleiert und ermöglichen es den Akteuren, bereits mit vergleichsweise geringen Kosten über beliebige Distanzen hinweg sofortige politisch-militärische Wirkung in der Grauzone unterhalb der Kriegsschwelle zu erzielen. Die beträchtlichen Investitionen in den Cyber-Bereich lassen auf eine zukünftig deutlich wachsende Eintrittswahrscheinlichkeit und ein erhöhtes Schadenspotenzial schliessen.

*Risiken und Bedrohungen im Cyberraum sind vielfältig und komplex: Sie reichen von kriminellen Aktivitäten zur Bereicherung über Spionage, Manipulation und Desinformation bis hin zum Einsatz offensiver Cybermittel in einem bewaffneten Konflikt. Um Gesellschaften zu destabilisieren oder zu schwächen, nutzen Angreifer immer häufiger Möglichkeiten, die sich aus der globalen Vernetzung und der Digitalisierung ergeben.*