Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Band: 98 (2023)
Heft: 7-8

Artikel: Sicherheit : im Dienst und ausser Dienst
Autor: Kienzi, Cécile
DOI: https://doi.org/10.5169/seals-1053001

Sicherheit: im Dienst und ausser Dienst

Im Dienst sorgen sich Kameradinnen und Kameraden um die Sicherheit der Truppe im Cyber-, elektromagnetischen- und Informationsraum. Mit nur wenig Aufwand kann jeder Soldat einen wichtigen Beitrag leisten. Wie sieht es dann im Zivilleben aus? Kann man dort auch mit einem Team die eigene Sicherheit verstärken?

Wm Cécile Kienzi

In erster Linie handelt es sich bei Cyberbedrohungen um ein relativ neues Risiko. Dies sowohl für Angehörige der Armee wie auch für Arbeitgeber, Selbstständige und Arbeitnehmer. Im Zentrum steht , im Zivilen und in der Armee, immer der Mensch.

Im Dienst

Die Cyber-, Informations- und elektromagnetischen Räume sind omnipräsent im Dienst. Egal, ob man nun mit Führungssystemen arbeitet oder etwa Panzermechaniker ist. In jeder Funktion und auf jeder Stufe muss man als Soldat auf Gefahren im Cyber-Raum achtgeben.

Die Armee hat dazu Cyber-Security-Regeln publiziert. Anbei ein kleiner Auszug:

Vorsicht vor privaten USB-Sticks!

Eine wichtige Regel in der Armee lautet: Niemals fremde oder private USB-Geräte an Systeme der Armee oder der Verwaltung anschliessen. Das bietet Angreifern eine Einfallmöglichkeit, um etwa Schadsoftware zu installieren. Auch das Aufladen von Smartphones soll nicht am PC geschehen, sondern nur via USB-Ladegerät.

Öffentliche Hotspots meiden

Wer mit Dienstgeräten (und auch mit privaten Geräten) unterwegs ist, sollte öffentliche Hotspots immer meiden. Ein manipuliertes Drahtlosnetzwerk ist einfach zu errichten und kann zum Verlust von Daten führen. Ein eigener Hotspot mit dem Handy ist sicherer.

Social Media

Wer Social Media richtig nutzt, kann viel zur Prävention beitragen. Die Gegenseite nutzt Social Media, um gezielt Informationen zu sammeln. Ob Datingplattform, Fitness-App oder Instagram – jede Information, die man preisgibt, ist grundsätzlich öffentlich abrufbar.

Im Dienst sollte man so wenig Informationen wie möglich preisgeben. Wenn zum Beispiel 30 User auf einmal regelmässig die gleiche Route joggen, kann das einen militärischen Standort preisgeben. Eine wesentlich sichere Alternative, um mit seinen Liebsten in Kontakt zu bleiben, ist und bleibt die Feldpost.

Zurück aus dem Dienst

Neben den präventiven Massnahmen gibt es in der Armee auch Spezialisten, die im Hintergrund zugunsten der Cybersicherheit arbeiten. Was nun, wenn man wieder zurück im Alltag ist? Wie soll man sich dort am besten verhalten und welche Schutzmöglichkeiten gibt es ?

Interview: Prävention ist Chefsache

Der SCHWEIZER SOLDAT hat bei Eric Zeller, Pressesprecher von Helvetia Versicherungen, nachgefragt wie es um Sicherheit und Prävention im Bereich Cyber im Berufsleben und im Alltag aussieht.

Herr Zeller, wie steht es um die Cyber-Hygiene von KMU? Braucht es unbedingt einen Spezialisten inhouse?

Eric Zeller: Es liegt auf der Hand, dass bei Einzel- oder Kleinstunternehmen nur selten ein spezifischer IT-Verantwortlicher definiert ist. Oftmals liegen die Datensicherung und Sicherung der entsprechenden Infrastruktur in den Händen von Drittanbietern. Gerade in diesen Fällen, aber auch bei Kundenunternehmen mit einer eigenen IT-Abteilung ist die präventive Absicherung gegen Cyberangriffe Chefsache.

Das heisst ein entsprechendes Konzept muss von der Geschäftsleitung nicht nur mitgetragen, sondern auch mitdefiniert und verantwortet werden.

Da aber auch die ausgefeiltesten Massnahmen nur einen bedingten Schutz versprechen, muss dem Risk Management und der allfälligen Bewältigung von Schadensszenarien verstärkte Priorität eingeräumt werden.

Eine Versicherung bietet keinen Ersatz für IT-Schutzmassnahmen, sondern dient als Ergänzung zu diesen. Bereits heute wird der Abschluss von Versicherungspolicen für Cyberrisiken immer mehr vom Vorhandensein technischer und organisatorischer Massnahmen abhängig gemacht.

Was kann man als Unternehmer im Bereich der Prävention tun?

Zeller: Der wichtigste Faktor beim Erkennen und Vermeiden von Cyber-Attacken ist immer noch der Mensch. Im Rahmen unserer Präventions- und Sensibilisierungsbemühungen fokussieren wir uns daher immer stark auf die Mitarbeitenden und versuchen unsere Kunden zu diesem Thema zu sensibilisieren.

Bild: VBS

Jeder kann im Dienst zur Sicherheit beitragen – dafür muss man sich aber an die Verhaltensregeln halten.

Zur Sensibilisierung der Mitarbeitenden bieten wir einfache, kostenlose Trainings an. Zudem ermöglicht unser kostenloser Cyber-Alert unseren Kunden, auf aktuelle Bedrohungen zu reagieren. Daneben bietet Helvetia Unternehmen auch Zugang zu einem Expertennetzwerk, wenn es etwa um die Implementierung von organisatorischen und technischen Massnahmen geht. Themen, die dabei immer wieder im Vordergrund stehen sind beispielsweise Back-up-Strategien, regelmässige Software-Updates (Patch Management) und das Handling von Zugriffsrechten.

✚ *Wie sieht es aus, wenn man sich als Privatperson schützen möchte?*

Zeller: Für Privatkunden bietet Helvetia seit 2019 Deckungen gegen Cyber-Risiken als Zusatz zur Privathaftpflicht- und zur Hausratversicherung an. Die Cyberdeckung hat sich in den vier Jahren seit der Einführung gut etabliert. Die Abschlusszahlen und damit auch das Prämienvolumen steigen jährlich, vorab aufgrund der immer stärker zunehmenden Nachfrage nach solchen Lösungen als Folge der Digitalisierung.

✚ *Was passiert in einem Schadenfall? Wie sollte man sich verhalten?*

Zeller: Helvetia Versicherungen empfiehlt ihren Kundinnen und Kunden im Falle eines Angriffes umgehend die die Unternehmenshotline (für Privatkunden) oder die 7/24-Cyber-Schadenhotline (für Firmenkunden) zu kontaktieren. Dort kann im Gespräch mit Experten das weitere Vorgehen und allenfalls die Meldung des Angriffes an die zuständigen Behörden (NCSC, Polizei, etc.) sowie eine allfällige Kontaktnahme mit den Urhebern des Angriffs abgeklärt werden. Je schneller eine derartige Meldung erfolgt, desto schneller kann eine anschliessende Schadensbeurteilung und -behebung in die Wege geleitet werden.

✚ *Vielen Dank für das Interview!*

Weitere Informationen sind unter folgendem Link zu finden:
www.helvetia.ch/cyber-versicherung

Neue Lösungen sind gefragt

Für Ereignisse, die über Einzelangriffe hinausgehen, also grossflächige (systemische) Cyber-Attacken, besteht im Bereich der finanziellen Kapazitäten in der Schweiz eine Lücke.

Angesichts des riesigen volkswirtschaftlichen Schadenpotenzials solcher Angriffe, stösst das Versicherungsprinzip des Ausgleichs an seine Grenzen. Hier sind weitergehende Lösungen gefragt, welche die bestehenden Lücken von der Vorsorge über die Schadenbewältigung bis zum finanziellen Ausgleich schliessen.

Nach Ansicht vieler Fachspezialisten kann daher die Versicherbarkeit solcher Grossrisiken nur mit einer dringlichen Gemeinschaftslösung unter Einbezug von Wirtschaft, Staat und Wissenschaft sichergestellt werden. ✚