Cyberbedrohung

Autor(en): **Jenni, Peter**

Objekttyp: **Article**

Zeitschrift: **Schweizer Soldat : die führende Militärzeitschrift der Schweiz**

Band (Jahr): **97 (2022)**

Heft 2

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-1005975

Cyberbedrohung

Am 26. Januar 2022 fand nach einem dreijährigen Unterbruch wegen der Pandemie der traditionelle Anlass des Handels- und Industrievereins des Kantons Bern (HIV) und der Offiziersgesellschaft der Stadt Bern (OGB) wieder statt. Anwesend waren in der Gstaad-Lounge im Stadion Wankdorf rund 200 Gäste.

Peter Jenni

Das Thema des Abends war die «Cyberbedrohung und der Umgang damit». Moderiert wurde der Anlass gekonnt von Sabine Gorgé von Radio SRF. Das Input-Referat hielt Yves Kraft von der Firma Oneconsult AG in Bern.

Es trug den Titel «Ransomeware heute». Kraft wies einleitend darauf hin, dass es wichtig sei, den Angreifer zu kennen. Nur so könne eine wirkungsvolle Verteidigung aufgebaut werden.

Er wies auch darauf hin, was Ransomeware ist: Sobald Daten auf dem Computer für den Benutzer nicht mehr verfügbar oder verschlüsselt seien, spreche man von eingedrungener Schadstoffsoftware. Erstmals dokumentiert wurde ein solcher Angriff im Jahr 1989 in den USA. Der Angreifer verlangte damals eine Zahlung von 189 Dollar.

Ransomeware heute

Das Ziel der Angreifer sei heute vielfach, dass der Betroffene oder eine Firma kompromittiert werde, dass sensible Daten entwendet würden, dass Daten verschlüsselt und allenfalls veröffentlich würden oder dass Personen an den Pranger gestellt würden.

Es bestehe auch die Gefahr, dass der Angreifer die Daten unbrauchbar mache, dass ein finanzieller Schaden bei Bezahlung des Lösegeldes drohe und dass die Firma gar in ihrer Existenz bedroht werde. Der Referent empfiehlt dringend, regelmässige Sicherung der Daten vorzunehmen und offline eine Sicherungskopie zu erstellen sowie das Schulen der Mitarbeiter im Umgang mit E-Mails.

Bei einem Angriff empfiehlt Kraft, wenn möglich den Schaden zu begrenzen, die Identifikation der infizierten Systeme, Strafanzeige, allenfalls forensische Untersuchungen, Sicherung der verschlüsselten Daten und Neuinstallation der betroffenen Systeme zu veranlassen und nichts zu bezahlen.

Aufbau des Kommando Cyber

Der mit dem Aufbau des Kommando Cyber der Armee beauftragte Divisionär Alain Vuitel informierte über die Gründe und den Umfang des Projektes. Ein Teil der Gründe liege in den beschriebenen Bedrohungen seines Vorredners.

Es gehe um deren Verhinderung in den Gebieten Daten, Personal, Infrastrukturen, Supply Chain und anderes mehr.

Ein wichtiger Zweck für den Aufbau des Cyber Kommandos sei die Bewahrung der Handlungsfreiheit. Am Beispiel einer Übersicht aus den USA mit 16 kritischen Infrastrukturen machte Vuitel deutlich, um was es geht.

Das Projekt Cyber der Armee begann 2021 mit der Formulierung der Grobstruktur. Zurzeit entstehe das eigentliche Konzept.

Im kommenden Jahr folge die Realisierung und 2024 die Einführung. Das Ziel sei, die Unversehrtheit der armeeeigenen IKT-Infrastruktur sicherzustellen und die Handlungsfreiheit während 24 Stunden an 365 Tagen zu bewahren.

Eine zentrale Rolle stelle in diesem Zusammenhang der neue Kampfjet F-35 dar. Damit werde die Datafusion ermöglicht, was die Wissens- und Entscheidungsfindung erleichtere.

In der Podiumsdiskussion wies Regierungsrat Philippe Müller, Sicherheitsdirektor des Kantons Bern, u.a. darauf hin, dass sein Polizeikorps in den kommenden Jahren personell verstärkt werde, um die vorhandenen Lücken aufzufüllen.

Auch die Polizei sei zunehmend mit Problemen von Ransomware konfrontiert. Sie müsse in der Lage sein, Private und Firmen im Kampf gegen Piraterie im Netz zu unterstützen.

V.l.n.r.: Oberst i Gst Frieder Fallscheer, Präsident Offiziersgesellschaft der Stadt Bern; Div. Alain Vuitel, PL Kdo Cyber; Yves Kraft, Oneconsult AG, Bern; Moderation: Sabine Gorgé, Radio SRF; Regierungsrat Philippe Müller, Sicherheitsdirektor des Kantons Bern; Dr. Adrian Haas, Direktor Handels- und Industrieverein des Kantons Bern.