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

Artikel: "Sicherheit bei Cyberangriffen gibt es nicht"
Autor: Christen, Elia
DOI: https://doi.org/10.5169/seals-1052987

«Sicherheit bei Cyberangriffen gibt es nicht»

Cyber-Security ist in aller Munde. Im Interview mit dem SCHWEIZER SOLDAT erzählt ein Cybersoldat, wie ein Cyberangriff auf die Armee aussehen könnte und warum auch er keine Lust auf komplizierte Passwörter hat.

Lt Elia Christen

Wie bist du Cybersoldat geworden?
Cybersoldat: Ich wusste frühzeitig, dass ich diesen Weg einschlagen möchte. So konnte ich meine Zeit in der Armee sinnvoll nutzen. Nachdem ich meine Rekrutenschule gestartet hatte, wechselte ich in den Cyber-Lehrgang, der 40 Wochen dauerte.

Hat dir die Cyberausbildung im zivilen Bereich geholfen?
Cybersoldat: Ich habe definitiv vieles gelernt, aber beruflich hilft mir die Ausbildung nicht weiter. Ich studiere nun etwas anderes. Für Informatiker oder Quereinsteiger, die sich im Bereich Cyber-Security weiter vertiefen möchten, ist dieser Lehrgang aber bestens geeignet.

Kann man sich aus jeder Funktion für den Cyber-Lehrgang bewerben?
Cybersoldat: Ja, das ist möglich. Jeder und jede startet zuerst in die Rekrutenschule. Ein Wechsel findet nach den ersten sechs Wochen statt, wenn die Selektion erfolgreich bestanden wurde.

Frauen haben sogar die Möglichkeit, zuerst die Aufnahmeprüfung zu versuchen, bevor sie sich für den Militärdienst einschreiben. Meiner Meinung nach wäre eine Aufnahmeprüfung vor der Rekrutierung auch für Männer sinnvoll. Denn es gibt einige Männer, die gerne eine Cyber-RS machen würden, aber aus Angst, nicht reinzukommen, in den Zivildienst wechseln.

Du bist jetzt im WK. Womit beschäftigst du dich da am meisten?
Cybersoldat: Wir unterstützen hauptsächlich das Personal der Bundesverwaltung. Mehr darf ich nicht sagen.

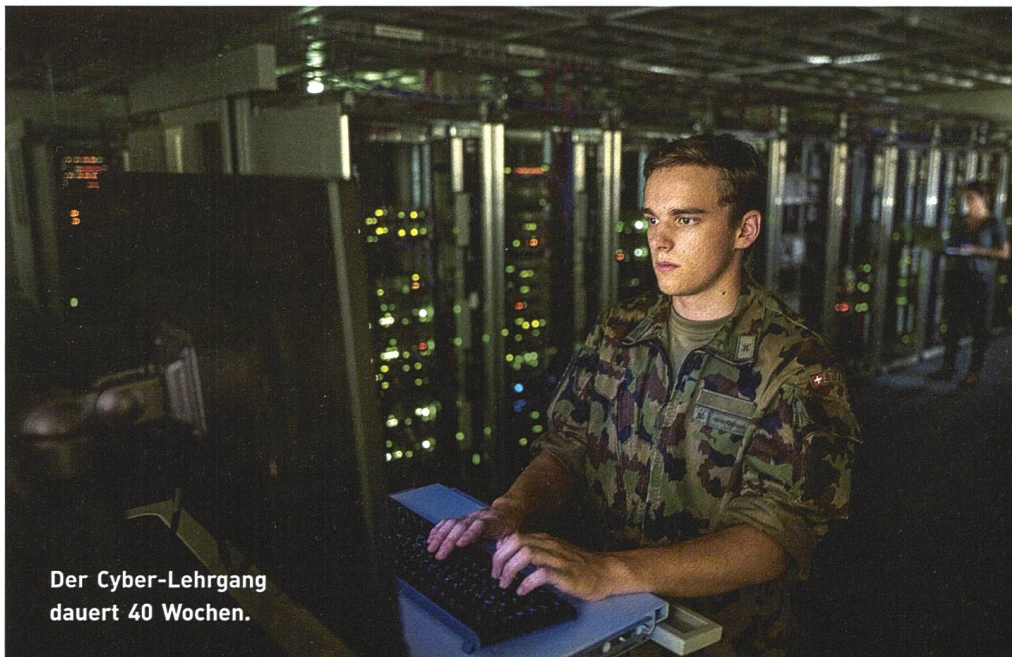
In letzter Zeit ist es auch bei Staatsbetrieben häufiger zu DDoS-Angriffen gekommen. Was ist das genau?
Cybersoldat: Das Ziel eines DoS (Denial of Service) ist, die Server zu überlasten, indem man sie mit Informationen überflutet. Heutzutage reicht eine einzelne Internetverbindung allerdings dafür nicht mehr aus. Jetzt haben wir den DDoS-Angriff (Distributed Denial of Service), bei dem mehrere Quellen auf einmal einen Server mit Anfragen überfluten.

Wie erkennt man einen DDoS-Angriff? Erst, wenn etwas offline ist?
Cybersoldat: Das wären die Auswirkungen bei einem erfolgreichen Angriff. Man kann jedoch auch Anomalien im Voraus erkennen. Wenn sich plötzlich Hunderte von Anfragen von ausländischen IP-Adressen häufen, entspricht das nicht dem normalen Muster. Wenn diese Anfragen dann auch noch in sehr kurzen Zeitabständen erfolgen, ist es besonders auffällig.

Ein DDoS-Angriff zielt also nicht direkt auf Informationen ab. Könnte er aber genutzt werden, um Schwachstellen zu schaffen und Informationen zu stehlen?
Cybersoldat: Ein standardmässiger DDoS-Angriff hat in erster Linie den Zweck, Schaden anzurichten. Man weiss jedoch nicht, ob dabei auch Informationen verloren gehen. Ein DDoS könnte

Cyberlehrgang

Der Cyberlehrgang dauert 40 Wochen und beinhaltet 800 Unterrichts- und Praxisstunden sowie einen Abschluss als Cyber Security Specialist EFA. Mehr Infos unter: miljobs.ch/functions/cybersoldat



Der Cyber-Lehrgang dauert 40 Wochen.

aber auch genutzt werden, um Schwachstellen zu schaffen. Informationsdiebstahl könnte dann ein weiterer Schritt sein.

✚ *Da sich solche Angriffe in letzter Zeit häufen: Wäre es an der Zeit, dass die Armee aushilft, zivile Infrastruktur zu schützen, ähnlich einer Katastrophenhilfe?*

Cybersoldat: Dafür braucht es enorme Ressourcen. Bei einer Überschwemmung siehst du, dass viel Wasser kommt, und du kannst reagieren. Im Cyberbereich ist das nicht so. Der Datenverkehr muss ständig überwacht werden. Du musst genügend Vorbereitungen treffen, um einen Angriff überhaupt erkennen zu können.

Wenn jemand deine Daten stiehlt, dann merkst du das nicht unbedingt, weil er ein exaktes Duplikat davon erstellen kann. Du erkennst es nur, wenn du ein entsprechendes Messgerät installiert und jemanden hast, der es bedient.

✚ *Ist die Armee selbst von Cyberangriffen betroffen?*

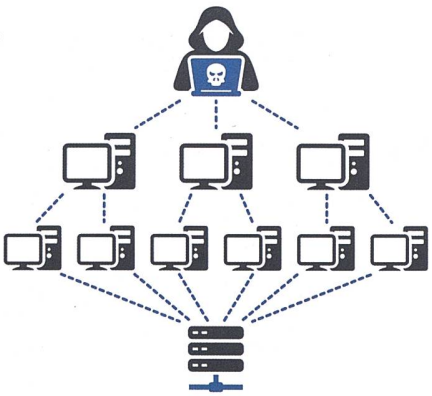
Cybersoldat: Das darf ich nicht beantworten. Cyber-Security funktioniert generell oft mit Verneinungen. Die Frage ist eher: «Wer ist nicht betroffen?» Man kann nicht sagen, dass wir sicher sind. Höchstens, dass wir nicht unsicher sind. Es ist ein Spiel mit Wahrscheinlichkeiten. Genauso kannst du nicht sagen: «Mein Gerät hat keinen Virus.» Du kannst eine ganze Woche lang danach suchen und am Ende kannst du nur wissen: «Ich habe keinen gefunden.»

✚ *Was könnten Motive für Angriffe auf die Armee sein?*

Cybersoldat: Zum einen können politische Interessen eine Rolle spielen. Aber es gibt auch andere Motive. Ähnlich wie bei einem Diebstahl einer Geldbörse kann es darum gehen, Geld zu benötigen oder Interesse an der Erbeutung von Identitäten zu haben. Es gibt aber auch Hacker, die das nur aus Interesse oder Spass machen.

✚ *Können Cyberangriffe ausschliesslich vom Bürotisch aus gestartet werden oder braucht es auch sozusagen «Boots on the Ground» oder Spione?*

Cybersoldat: Die heutigen Systeme sind extrem komplex. Ein Hacker kann nicht



Bei einem DDoS-Angriff (Distribued Denial of Service) überfluten mehrere Quellen einen Server mit Anfragen, um diesen zu überlasten.

mehr ein ganzes Gerät beherrschen, deshalb muss er sich auf einen bestimmten Bereich spezialisieren. Beim iPhone gibt es beispielsweise Experten, die nur auf den PIN-Code spezialisiert sind. Um den PIN-Code von jemandem herauszufinden, ist es also viel einfacher, sich einfach im Zug neben ihn zu setzten und zu beobachten, wie er den PIN eingibt.

✚ *Was sind die am häufigsten verwendeten Methoden?*

Cybersoldat: Social Engineering wie das Beobachten des PIN-Codes oder Passwortes, Keylogger, Abhören, Phishing oder Vishing (Voice Phishing) sind sehr häufig.

Ihr kennt sicher das Video von Cedric Schild des Online-Magazins «Izzy Magazine», in dem er auf einer Wache anruft und sich als ein Offizier ausgibt. Mit nur einem Anruf hat er einfach so den Wachtplan bekommen. Er hätte bestimmt noch mehr erreichen können.

✚ *Abgesehen von diesem Beispiel: Ist das schon einmal in der Armee vorgekommen?*

Cybersoldat: Ich kann eine interessante Geschichte aus einer Cyber-Übung erzählen: Im Rahmen einer Simulation wurde ein höherer Stabsoffizier gehackt. Alle Versuchsteilnehmer wussten, dass sie in den nächsten Wochen vielleicht Ziel eines Cyberangriffes werden.

Trotz der Vorsicht haben die Angreifer es geschafft: Via Amazon haben sie eine grosse Anzahl an Blumentöpfen an die Privatadresse des Ziels bestellt. Diese standen dann da einige Zeit herum. Anschliessend schickten sie einen falschen Amazon-Mitarbeiter vorbei, um die Ware wieder abzuholen. Als «Entschuldigung» schenkte der dem Opfer einen kleinen USB-betriebenen Ventilator. Das passte ganz gut, denn es war ein sehr heisser Sommer. Der Ventilator war natürlich präpariert. Es dauerte nicht lange, bis dieser Ventilator an ein Gerät angeschlossen wurde und die Angreifer die Kontrolle übernehmen konnten. Erratest du, wer die wichtigste Person bei der Aktion war?

✚ *Die Hacker?*

Cybersoldat: Nein. Der Filmregisseur (lacht).

✚ *Interessant. Würdest du also sagen, dass das grösste Risiko für einen Angriff der Endnutzer ist, der nicht gut genug weiss, wie man sich schützt?*

Cybersoldat: Der Endnutzer ist sehr vulnerabel. Man kann ihn zum Beispiel mit Phishing oder ähnlichen Methoden angreifen. Und es geht dabei nicht um dich persönlich, sondern um dein Gerät.

✚ *Warum ist das Gerät so interessant?*

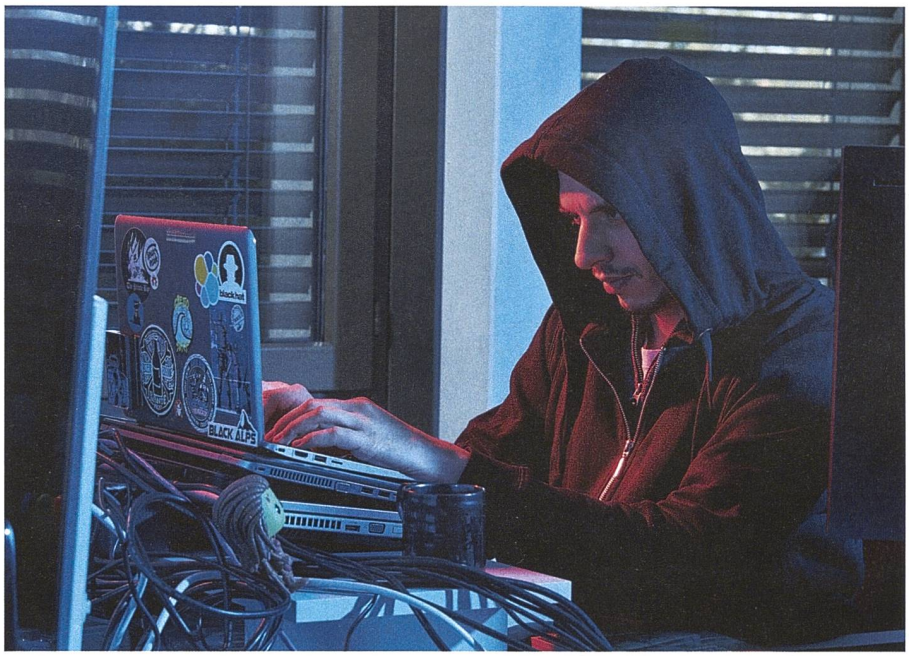
Cybersoldat: Heutzutage enthalten private Geräte sehr viel persönliches Leben. Wenn deine Apple-ID gestohlen wird, hast du ein massives Problem. Vielleicht hast du Apple Pay oder Twint oder ähnliches. Es gibt enorm viele Informationen darin.

✚ *Würdest du sagen, du selber könntest darauf hereinfallen, wenn so ein Angriff perfekt wäre?*

Cybersoldat: Ja, sofort. Sogar, wenn er nicht perfekt wäre. Denn sonst müsste ich

Bilder: VBS

Ein präparierter USB-Stick reicht aus, um auf die Daten eines Geräts zugreifen zu können.



Die häufigste Form von Cyber-Attacken ist nicht etwa der klassische Hackerangriff, sondern Social Engineering (Symbolbild).

paranoid durch diese Welt laufen. Ein Angriff könnte von überall kommen. Mich kann das genauso treffen wie dich. Egal, wie gut man vorbereitet ist, man ist nie unverwundbar. Opfer von einem simplen Angriff kann man dennoch werden.

Sind deine Passwörter sicherer als meine?

Cybersoldat: Nein. Warum hast du unsichere Passwörter? Aus Bequemlichkeit. Auch ich bin bequem. Jemand mit wenig Erfahrung ist möglicherweise weniger geschützt, aber mein Gerät ist sicherlich nicht besser geschützt als deines.

Wenn eine Organisation im Visier eines Angreifers ist: Hilft es, wenn man dafür sorgt, dass man nicht das schwächste Tier im Rudel ist?

Cybersoldat: Die Stärke einer Kette ist definiert durch das Schwächste Glied. Es geht nicht um Rudel, sondern um Ketten.

Ein Beispiel für das schwächste Glied in der Kette ist die Sicherheit eines Unternehmensnetzwerks. Wenn eine Schwachstelle, wie eine veraltete Firewall, ausgenutzt wird, kann ein Angreifer das gesamte Netzwerk kompromittieren, unabhängig von anderen Sicherheitsmassnahmen. Es ist wichtig, alle Teile der Sicherheitskette zu schützen, um solche Risiken zu minimieren.

Also hilft es nur etwas, wenn alle gut geschützt sind?

Cybersoldat: Damit maximierst du den Gesamtschutz, das ist wichtig. Ein Angreifer muss zuerst das schwächste Glied identifizieren. Je weniger schwache Glieder es gibt, desto schwieriger ist es, ein anfälliges Teil zu entdecken. Das ist die Idee.

Sind die E-Learning-Lektionen eine wirksame Massnahme gegen Cyberangriffe?

Cybersoldat: Nicht wirklich. Was ist deine Erfahrung mit LMS (Learning Management Systemen)?

Durchklicken …

Cybersoldat: Da haben wir es. Egal, welchen Grad du hast, es wird durchgeklickt.

Wie könnte man das verbessern?

Cybersoldat: Man könnte die Cyber-Awareness aller Soldaten verbessern, egal welcher Funktion. Und zwar mit Ausbildungen von Cyber-Experte zu AdA.

Vielleicht mit einer Cyberausbildung, direkt integriert in die Allgemeine Grundausbildung. Dort könnten die Rekruten lernen, sorgfältig mit ihren Daten umzugehen und die potenziellen Risiken zu kennen.

Vielen Dank für das Interview.