ICT BERUFSBILDUNG AARGAU

ZUSAMMENARBEIT FÜR MEHR KNOW-HOW ZU CYBERCRIME IN DER BERUFSBILDUNG

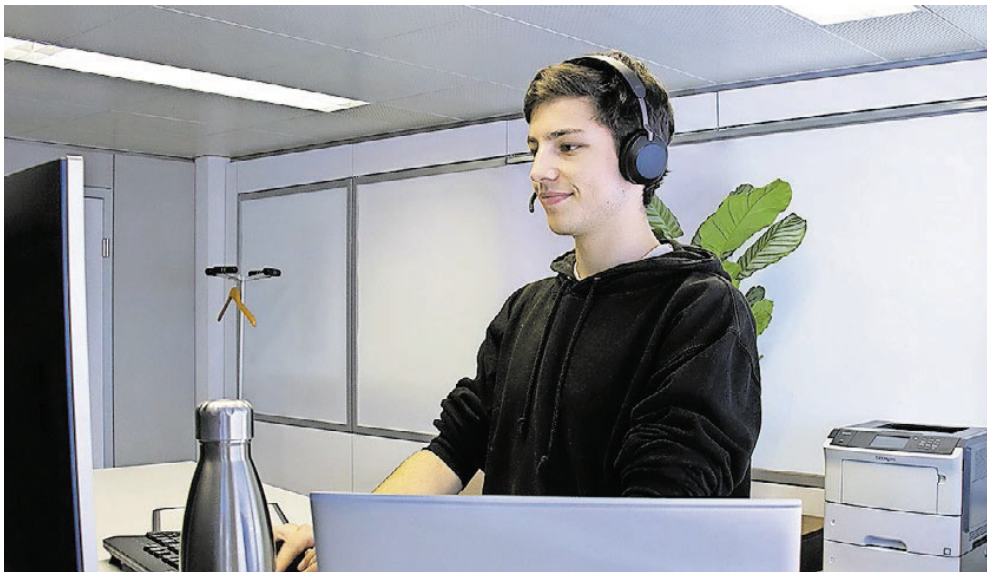
Hacking hat sich in den letzten Jahren hin zu einem normalen Geschäftsmodell krimineller Organisationen und Einzelpersonen gewandelt. Angriffe diverser Art können «as a Service» gekauft werden, der Verkauf von Angriffstools, Viren und gestohlenen persönlichen Daten auf illegalen Marktplätzen ist ein Milliardengeschäft.

ICT BERUFSBILDUNG AARGAU

Umso wichtiger ist es, dass schon Lernende aus allen Branchen in ihrer Berufsausbildung erfahren, wie sie sich und ihre Arbeitskolleg*innen vor Hacking schützen können. Aus diesem Grund unterstützt ICT Berufsbildung Aargau das EU-finanzierte Projekt GEIGER, welches eine auf die KMU zugeschnittene Lösung entwickelt. GEIGER bietet:

- laufend aktualisierte Informationen über persönlich relevante Cyber-Bedrohungen
- personalisierte Empfehlungen zur Minimierung der Risiken für KMU angesichts der Bedrohungen
- Zugang zu den jeweils am besten geeigneten Tools für Schutz, Reaktion und Schulung
- Schulung und Zusammenführung von Cybersecurity-Spezialisten

Diese vier Punkte zeigen auch unabhängig von diesem Projekt, die für eine umfassende Sicherheit benötigten Handlungsbereiche. Das Projekt wird durch FHNW geführt und koordiniert. Die Berufsfachschule BBB übernimmt die Entwicklung von Ausbildungsinhalten mit dem Ziel, allen Berufslernenden aus allen Branchen grundlegende Kompetenzen im Bereich Cybersecurity zu vermitteln (https://project.cyber-geiger.eu/).



Lernende aus den ICT Berufen werden gezielt auf Cyber-Bedrohungen geschult.

Statements von Lernenden

Lisa und Angelina machen eine Lehre als Coiffeusen EFZ und sind im 2. Lehrjahr. Sie haben im Juni im Rahmen des Projekts GEIGER eine Ausbildung zu Cybersecurity-Defender begonnen.

Lisa: «Ich interessiere mich für Cybersicherheit, da man sich heute ein Leben ohne Medien nicht mehr vorstellen könnte. So müssen wir wissen, wie wir unsere Geräte richtig schützen können. Und über diesen Schutz will ich mich genauer informieren. Im Geschäft haben wir noch nie wirklich über Cybersicherheit geredet.»

Angelina: «Cybersicherheit ist ein Thema, das mich (uns alle) fast täglich betrifft. Wir alle müssen uns damit herumschlagen. Es ist wichtig zu wissen, wie man sich schützen kann. Im Geschäft machen wir regelmässig Updates und haben Virenschutzprogramme auf unseren Laptops installiert. Jedoch ist es sonst kein grosses Thema bei uns, das Bewusstsein fehlt.»

Auch die Lernenden in verschiedenen ICT Berufen machen sich mit dem Thema immer vertrauter und erweitern ihr Wissen stetig, wie die Statements zeigen:

Timeo: «Vieles wusste ich schon, da das Thema heutzutage jeder kennen sollte. Einige Sachen habe ich aber auch im ÜK, in der Schule und im Betrieb gelernt und das Ganze zusammen ergibt dann mein Wissen.»

Patrick: «Cyber Security wird in unserem Arbeitsfeld immer wichtiger, die Methoden von Hackern werden komplexer und jeder muss immer mehr auf der Hut sein. Bei uns im Geschäft gibt es strenge Richtlinien bezüglich Passwörtern, aber auch der Umgang mit Spam-Mails ist geregelt und problematische Webseiten sind in unserem Netzwerk gesperrt. Mit diesen Massnahmen trägt jeder zum digitalen Schutz unseres Unternehmens bei, was auch entscheidend ist, da der Mensch im Bereich Cyber Security das schwächste Glied der Kette bildet.»

Kalid: «Ich habe grossen Respekt davor, Zugang zu meinen Konten zu verlieren, und verhalte mich deswegen generell vorsichtig in meinem

ICT Berufsbildung Aargau fördert die Aus- und Weiterbildung der Lernenden der ICT-Berufe im Aargau, indem alle Interessengruppen der beruflichen Aus- und Weiterbildung in diesem Bereich zusammengebracht werden. Die attraktiven Lehrberufe Informatiker*in, Mediamatiker*in, ICT-Fachleute und künftig auch Entwickler*in Digitales Business sind gefragter denn je. Die Nachfrage bei den Jugendlichen ist riesig und der Fachkräftemangel zeigt auf, dass künftig noch viel mehr Leute in diesen Berufsfeldern ausgebildet werden müssen. Wir arbeiten sowohl mit den Berufsfachschulen, den Ausbildner*innen, den Arbeitgeber*innen, dem Kanton als auch den Lernenden und Arbeitnehmer*innen zusammen.

digitalen Umfeld. Zum Beispiel benutze ich 5-Minuten-E-Mails, wo ich nicht zwingend meine echte Mail angeben muss, und verwende einen Passwortmanager, sofern möglich. In den letzten Jahren ist das Thema für mich deutlich mehr in den Vordergrund gerückt. Ich bin froh, mit meinem IT-Background vieles ableiten zu können, sonst wäre ich wahrscheinlich verloren.»

Eine angehende Mediamatikerin erläutert ihre Projektorganisation.

Noch kaum Fortschritte feststellbar

Dass sich Unternehmen und Mitarbeitende der Gefahren noch nicht richtig bewusst sind, zeigen auch zwei Studien des gfs-Zürich[1] und der ZHAW[2]. Erstere kommt zum Schluss, dass in den letzten Jahren keine Fortschritte bezüglich der Umsetzung von Cybersicherheitsmassnahmen festgestellt werden konnte, obschon das Thema in den Medien viel präsenter geworden ist und auch die Unternehmen das Risiko, von einem Cyberangriff betroffen zu werden, mittlerweile höher einschätzen. Die Studie der ZHAW bescheinigt den KMU positive Elemente. Nebst den gängigen Empfehlungen zur Absicherung der Infrastruktur kann die Wirkung insbesondere durch die Umsetzung der folgenden Massnahmen verstärkt werden, die relativ einfach und ohne grosse Investitionen von jedem KMU umgesetzt werden können.

Workshop in Mägenwil

ICT Berufsbildung Aargau zeigt zusammen mit dem ICT LearnHub in Mägenwil in einem Kurs auf, welche Gefahren aus dem Internet drohen und was man dagegen tun kann. In einem eigentlichen Workshop-Teil helfen wir, die Bedrohung für Unternehmen konkret einzuschätzen.

Mehr Informationen: www.ict-learnhub.ch/cyberkmu

1 https://digitalswitzerland.com/wp-content/uploads/2022/06/Schlussbericht_CyberriskKMU2022_final.pdf / Juni 2022

2 https://www.zhaw.ch/storage/sml/institute-zentren/iri/upload/2021_Pugnetti-Casian_Cyberrisiken-und-Schweizer-KMU.pdf

Kriminelle Cyberangreifer verdienen ihr Geld grundsätzlich auf folgende vier Arten.*

Diebstahl und Verkauf von persönlichen Daten:
Die Erstellung einer Phishing-Seite, die ein beliebtes soziales Netzwerk imitiert, und die Einrichtung einer Spam-Massensendung mit einem Link zu der gefälschten Website kostet durchschnittlich 150 CHF. Wenn die Benutzer 100 Personen erwischen, können sie durch den Verkauf sensibler Daten bis zu 10 000 CHF einnehmen. Die Opfer verlieren im Gegenzug ihre wertvollen Kontakte, persönlichen Fotos und Nachrichten.

Erpressung durch den Diebstahl von Systemzugriffen:
Ein mobiler Trojaner-Blocker ist wesentlich teurer – der Kauf und die Verbreitung der Schadsoftware kostet im Durchschnitt 1000 CHF. Allerdings ist der «Gewinn» auch viel höher. Die Preise, die die Angreifer für die Entsperrung eines Smartphones verlangen, variieren zwischen 10 und 200 CHF, was bedeutet, dass sie von 100 potenziellen Opfern bis zu 20 000 CHF erhalten können.

Erpressung durch den Diebstahl von Datenzugriffen:
Die gleiche Summe kann mit verschlüsselnder Ransomware verdient werden, aber die «Anfangsinvestition» ist doppelt so hoch – etwa 2000 CHF. Die Verluste der Nutzer sind ebenfalls höher, da die Betrüger als Mindestbetrag für die Entschlüsselung der Daten in der Regel 100 CHF verlangen.

Diebstahl durch den Zugang zum Bankkonto
Um den Jackpot zu knacken, suchen die Betrüger nach Banking-Trojanern, die direkt auf Geld abzielen. Nachdem sie etwa 3000 CHF für die Malware, den Exploit und eine Spam-Mail zur Verbreitung ausgegeben haben, können die Cyberkriminellen bis zu 72 000 CHF erbeuten. Der durchschnittliche Verlust eines einzelnen Opfers beträgt 722 CHF.

In den Medien werden erfolgreiche Angriffe regelmässig thematisiert, dennoch ist das Thema Cybersecurity für KMU kein einfaches, Dienstleister sind teuer, mit der Cyberversicherung allein ist es noch nicht getan und eine regelmässige Weiterbildung nebst dem Tagesgeschäft liegt auch fast nicht drin.

*Diese vier Beispiele stammen von Kaspersky (https://www.kaspersky.com/about/press-releases/2014_the-hackers-bounty-how-much-do-cybercriminals-make-from-innocent-users), 2014, gelten aber laut Angaben des Unternehmens grundsätzlich auch heute noch.