Schutzmaßnahmen erhöhen

Bedingt durch die Corona-Pandemie, verlagerten sich viele Dinge aus dem realen Leben in die virtuelle Welt. Kriminelle nützen dies aus, weshalb mehr denn je auf Cyber-Sicherheit geachtet werden muss.

In Zeiten, in denen die eigenen vier Wände zum zentralen Lebensmittelpunkt wurden, sind Internet, Smartphone, Computer oder Spielekonsole für den Alltag vieler Menschen wichtig geworden. Das Internet wird nicht nur zum Arbeiten, sondern auch vermehrt für Onlineshopping, Onlinebanking sowie Gaming oder Streaming genutzt.

Kaspersky-Umfrage. Um herauszufinden, wie die Nutzerinnen und Nutzer ihr Risiko, Opfer eines Cybercrime-Delikts zu werden, einschätzen, führte der Antivirus-Software-Anbieter *Kaspersky* im Mai 2020 eine internationale Umfrage unter mehr als 10.000 Nutzerinnen und Nutzern durch, die mindestens zwei im Haushalt vernetzte Geräte nutzen. Im deutschsprachigen Raum (DACH-Region) wurden 1.010 Nutzerinnen und Nutzer befragt, darunter 506 Deutsche, 251 Österreicher und 253 Schweizer.

Viele Menschen nutzen in der Corona-Krise im Homeoffice vermehrt das Internet, machen sich aber wenig Gedanken über Risiken bei der Nutzung.

Ergebnisse. Wie die Ergebnisse zeigen, haben sich die privaten Tätigkeiten von 75 Prozent der Befragten aus dem realen Leben in das Internet verlagert. 45 Prozent der Nutzerinnen und Nutzer halten aufgrund der Beschränkungen online Kontakt zu ihren Freunden und Angehörigen. 23 Prozent der Umfrage-Teilnehmerinnen und -Teilnehmer im DACH-Raum gaben an, Bankwege nun lieber online zu erledigen, als in die Filiale zu gehen.

Auch der stationäre Handel ist zum Teil sehr stark von Einschränkungen betroffen, weshalb vermehrt in Onlineshops eingekauft wird: 36 Prozent ziehen den Einkauf im Web dem Geschäft vor. Ein Problem stellt die Verwendung von privaten Geräten zu Homeoffice-Zwecken dar. 68 Prozent der weltweit Befragten verwenden ihre privaten Geräte, wie Laptops zur Erledigung von Arbeitsaufträgen, was von anderen aktuellen *Kaspersky*-Untersuchungen belegt wird. Obwohl die Internetnutzung zu Hause seit der Corona-Krise und den damit verbundenen Einschränkungen bei fast der Hälfte der Nutzerinnen und Nutzer (45 Prozent) in der DACH-Region um mindestens zwei Stunden pro Tag gestiegen ist, denkt mehr als jeder Dritte (37 Prozent), dass er keinem großen Risiko ausgesetzt ist, Opfer einer Cyber-Attacke zu werden.

Doxing- und Brute-Force-Angriffe. Wie Beispiele zeigen, sind Privatanwenderinnen und -anwender von Betrug und Unternehmen zunehmend von Doxing-Angriffen betroffen. Dabei werden persönliche Daten abgesaugt, um Personen anschließend zu erpressen. Ein neuer Trend zeigt, dass vermehrt Unternehmen von Doxing betroffen sind. Weiters wurde eine ansteigende Anzahl an Brute-Force-Attacken auf Remote-Desktop-Protocol-Tools (RDP-Tools) festgestellt. *Kaspersky*-Experten sehen dieser Entwicklung mit Sorge entgegen, da sich die Angreiferinnen und Angreifer über Geräte im Homeoffice einen einfachen Zugang zu Unternehmensnetzwerken verschaffen können. Zwischen April und Oktober 2020 konnten im DACH-Raum 205.739.438 versuchte Angriffe auf RDP-Tools registriert werden.

„Vor allem das Remote Desktop Protokoll für den Fernzugriff ist im Visier der Angreifer. Allein im September gab es in Österreich 6.408.607 versuchte Angriffe“, erklärte Christian Funk, Leiter des Forschungs- und Analyse-Teams in der DACH-Region bei *Kaspersky*. „Agiert der Mitarbeiter fahrlässig oder ist die IT-Abteilung zu leichtsinnig, bekommt der Angreifer einfachen Zugriff über den Laptop des Mitarbeiters ins Unternehmensnetzwerk. Da bei der Heimarbeit für die private und berufliche Nutzung häufig dasselbe Gerät genutzt wird, birgt das ein erhebliches Sicherheitsrisiko“, führte der Experte weiter aus.

Geringeres Risikoempfinden. Das Ziel der Umfrage war es, herauszufinden, wie sicher sich die Nutzerinnen und Nutzer der DACH-Region bei beispielsweise sensiblen Transaktionen, wie Onlineshopping oder Onlinebanking fühlen. Die Ergebnisse zeigen, dass sich 29 Prozent der Befragten wenig um die Sicherheit des Internets zu Hause sorgen. Sobald es um kritische Bereiche und wertvolle Daten geht, machen sich 66 Prozent Gedanken über ihre Sicherheit.

Eine Langzeitanalyse von *Kaspersky* spiegelt ebenfalls wider, dass das Sicherheitsbewusstsein im internationalen Vergleich geringer ausgeprägt ist: 2019 wurden in Deutschland 21 Prozent aller weltweiten Banking-Malware-Angriffe verzeichnet, ein Anstieg um den Faktor 3 im Vergleich zum Vorjahr (7 Prozent aller weltweiten

FOTO: PRESSMASTER/STOCK.ADOBE.COM

Attacken). Zudem stellte sich heraus, dass es die Mehrheit der Phishing-Angriffe (52 Prozent) zielgerichtet auf Finanzangelegenheiten, wie Onlinebanking, E-Paymentsystem-Nutzer und Onlineshopper abgesehen hat. „Phishing ist für Cyberkriminelle eines der Standbeine schlechthin – technisch einfach in der Durchführung, massenhafte Verbreitung und damit hohe Erfolgschancen – unabhängig vom eingesetzten Betriebssystem“, erklärte Funk.

Schutz durch Passwörter. Cyber-Kriminelle haben insbesondere Zugänge und Zahlungsdaten, wie Kreditkartendaten im Visier. Um sich und seine Daten bestmöglich zu schützen, sind passwortgeschützte Geräte, wie Laptops oder Smartphones unerlässlich, jedoch gerät das eigene WLAN bei 38 Prozent der Befragten in Vergessenheit. 62 Prozent geben an, das private WLAN mit einem Passwort gesichert zu haben. Da diese Sicherheitslücke nicht nur von Nachbarn ausgenutzt werden kann, sondern auch Kriminellen ein Einfallstor bietet, muss auch in diesem Punkt auf einen Schutz geachtet werden.

„Die Nachfrage nach Smart-Home-Geräten steigt und sie sind dadurch attraktive Ziele für Cyber-Kriminelle. Wenn diese durch ein ungesichertes WLAN Kontrolle über die Geräte erlangen, kann das unangenehme Folgen haben“, betonte Funk. Die Lösung ist so einfach wie effektiv: Ein ordentliches und konsequentes Passwortmanagement. Ein gutes Passwort sollte aus mindestens acht Zeichen bestehen, aber je mehr, desto besser und Groß- sowie Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Das regelmäßige Ändern wird auch empfohlen.

Bundeskriminalamt warnt vor zunehmender Cyberkriminalität. Die Entwicklungen im Cybercrime-Bereich zeigen einen alarmierenden Trend: Im Jahr 2019 wurden 28.439 Straftaten angezeigt, ein Plus von 44,9 Prozent im Vergleich zum Vorjahr. Mit mehr als 59 Prozent der angezeigten Fälle (16.831 Anzeigen) ist der Internetbetrug, gerechnet auf den gesamten Cybercrime-Bereich, auf Platz 1.

Das Bundeskriminalamt veröffentlicht unter anderem in regelmäßigen Abständen Warnungen und Präventionstipps, um die Bevölkerung über (neue) Betrugsmaschen oder Trends zu informieren und den richtigen Umgang mit dem Thema Cybercrime und Sicherheit näher zu bringen. Denn nur, wenn man die Vorgehensweisen und Absichten der Täter kennt, kann das Risiko Opfer eines Cybercrime-Delikts zu werden, reduziert werden.

Weitere Informationen gibt es unter: *www.bundeskriminalamt.at,* unter Präventionstipps.

Europol-Kampagne für mehr Sicherheit. Das Thema Cyber-Sicherheit im Homeoffice beschäftigt nicht nur das Bundeskriminalamt, sondern auch Europol. Da viele Unternehmen auf Homeoffice umstellen mussten und die Unternehmenssicherheit nicht immer im ausreichenden Maße gewährleistet ist, startete Europol eine Informationskampagne, um Unternehmerinnen und Unternehmer sowie Mitarbeiterinnen und Mitarbeiter für dieses Thema zu sensibilisieren.

Neben dem Thema Homeoffice steht der richtige und sichere Umgang mit der digitalen Welt im Fokus. So soll der Schutz vor Cyber-Angriffen und die Sicherheit beim Onlineshopping forciert und vor Phishing-Mails und den Gefahren für Kinder und Jugendlichen im Netz gewarnt werden.

Weitere Informationen: www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/safe-teleworking-tips-and-advice

Romana Tofan

SICHERHEITSMANAGEMENT UND CYBERSECURITY

Cyber-Kompetenz für HAK-Schüler

Die polizeiliche Kriminalstatistik 2019 zeigt, dass die Zahl der Delikte von Hacking und Datenmissbrauch um 150 Prozent gegenüber 2018 zugenommen hat. Die Zahl der Betrugsdelikte im Internet stieg auf 16.831. Das ist der höchste Wert der letzten Jahre.

Federführend haben der ehemalige Landespolizeidirektor von Salzburg Dr. Franz Ruf (seit Juni 2020 Generaldirektor für öffentliche Sicherheit) und der Schulleiter der BHAK Tamsweg, Direktor Mag. Herbert Giegerl, einen neuen Ausbildungszweig „Sicherheitsmanagement und Cybersecurity“ *(management.cyber.security)* kreiert.

Ab dem Schuljahr 2021 werden Schülerinnen und Schüler der BHAK Tamsweg zu Expertinnen und Experten im Bereich Sicherheitsmanagement und Cybersecurity ausgebildet. „Wir

Schülerinnen und Schülern der BHAK Tamsweg werden ab dem Schuljahr 2021 Cyber-Sicherheitskompetenzen vermittelt.

wollen Jugendliche früh über den Umgang mit dem Internet sensibilisieren. Es beginnt bei sozialen Medien, Internetbetrug und geht bis hin zu Cybercrime im Darknet“, berichtet Direktor Giegerl.

Unterrichtsgegenstände des Moduls „management.cyber.security“ sind unter anderem „Sicherheitsmanagement“ (Bedrohungsszenarien, Krisenmanagement, Korruptionsbekämpfung, Schutz kritischer Infrastruktur) und „Cybersecurity“ (Internetbetrug, Umgang mit sozialen Medien, Cybermobbing, Cybergrooming, Phishing, Malware, Cyber-Attacken, Hackerangriffe, Darknet). Die praxisbezogene Ausbildung bindet Expertinnen und Experten der Landespolizeidirektion Salzburg, des Sicherheits- und Katastrophenschutzes des Landes Salzburg sowie des Landeskriminalamts ein. Zusatzausbildungen zum Brandschutzbeauftragten und die Stabsausbildung runden die Ausbildung ab.

Den Schülerinnen und Schülern steht ein eigenes, modernes Schülerheim in unmittelbarer Nähe der Schule zur Verfügung. „Wir sprechen junge Menschen an, die sich für eine Karriere im Polizeidienst oder als Sicherheitsexperte im privatwirtschaftlichen Sicherheitsdienst interessieren“, sagt Direktor Giegerl.

Weitere Informationen unter www.haktamsweg.at.

FOTO: KWER