

Risiko CYBERKRIMINALITÄT

Seit Oktober 2019 gibt es bei der Kantonspolizei Schwyz den Fachbereich Cybercrime. In der Zentralschweiz sind zwei Kantonspolizeien (Zuger Polizei und Kantonspolizei Schwyz) vom Bundesamt für Kommunikation anerkannte Stellen für die Bekämpfung der Cyberkriminalität. Seit der Schaffung leitet Valentin Bonderer diesen Fachbereich mit aktuell zwei spezialisierten Mitarbeitern. Er gibt uns im Interview Einsicht in seine Erfahrungen sowie Tätigkeiten und gibt Ratschläge, wie das Risiko eines Betrugs minimiert werden kann.



Valentin Bonderer,
Leiter Fachbereich
Cybercrime, Stv. Chef
Dienst Wirtschaftsdelikte und Cybercrime Kantonspolizei Schwyz

Womit befasst sich der Fachbereich Cyberkriminalität der Kapo Schwyz?

Aufgrund der zunehmenden Digitalisierung betrifft die Cyberkriminalität zahlreiche Lebensbereiche und umfasst die ganze Bevölkerung. Der volkswirtschaftliche Schaden, der durch Cyberkriminalität verursacht wird, ist sehr gross. Die Öffentlichkeit erwartet deshalb von den Strafverfolgungsbehörden, dass diese Delikte effektiv und effizient verhindert, verfolgt und geahndet werden. Wir ermitteln gegen alle Formen der Internetkriminalität. Mit Prävention und Repression sorgen wir für mehr Sicherheit im virtuellen Raum.

Welche Art von Cyberkriminalität wird am häufigsten angezeigt?

Weit verbreitet sind der Bestellbetrug (Betrug auf Kleinanzeigen-Plattformen) und der Online-Anlagebetrug. Beim Bestellbetrug wird zum Beispiel auf Portalen wie Anibis.ch oder ricardo.ch ein iPhone angeboten. Der Käufer bezahlt zwar, erhält den angepriesenen Gegenstand aber nie. Die Schadenssumme im Bereich Online-Anlagebetrug belief sich im Kanton Schwyz im Jahr 2019 auf fast 9 Millionen Franken. Diese Masche funktioniert folgendermassen: Der Geschädigte investiert Geld in eine Firma, das mit «hoher Rendite» angelegt wird, das Geld ist dann jedoch weg.

Auch vor Ransomware-Angriffen werden wir im Kanton Schwyz nicht mehr verschont. Unter Ransomware versteht man eine spezielle Art schädlicher Software, die den Zugriff auf Geräte sperrt oder darauf enthaltene Daten verschlüsselt. Anschliessend wird vom Opfer ein Lösegeld für die Wiederherstellung verlangt. Es finden immer mehr solche Angriffe statt und die Dunkelziffer ist deutlich grösser als die bekannte Melderate. Neu ist an dieser Masche, dass die Angriffe gezielt erfolgen. Die Ransomware-Angriffe richten sich gegen Unternehmen aus allen Branchen und jeder Grösse.

ÖFFENTLICHKEITSVERANSTALTUNGEN

Die Fachstelle Cybercrime der Kantonspolizei Schwyz führt zwei öffentliche Veranstaltungen zum Thema Cybercrime durch:

- 30. September 2021, 19.00 Uhr,
Monséjour Zentrum am See in Küsnacht am Rigi
 - 28. Oktober 2021, 19.00 Uhr,
Zwei Raben Kultur- und Kongresszentrum in Einsiedeln
- Weitere Informationen erhalten Sie unter www.sz.ch/polizei und cybercrime.polizei@sz.ch

Wie können sich Unternehmen und Privatpersonen vom Risiko eines Cyberangriffes oder -betrugs schützen?

Komplett vor Cyberangriffen können sich Unternehmen und Private nicht schützen, aber mit einigen einfachen Punkten kann man das Risiko deutlich verringern. Als Erstes sollte man sichere Passwörter verwenden. Sichere Passwörter sollten mindestens 12 Zeichen lang sein, aus Gross- und Kleinbuchstaben sowie Sonderzeichen bestehen und in keinem Wörterbuch zu finden sein oder nicht mit der Person in Verbindung stehen. Wichtig ist auch, dass man für unterschiedliche Dienste verschiedene Passwörter hat. Damit man den Überblick behält, empfiehlt es sich, einen Passwortmanager einzusetzen.

Eine zentrale Rolle im Bereich IT-Sicherheit kommt dem Menschen zu, er ist aber auch der grösste Risikofaktor. Hacker versuchen in Systeme von Firmen und Privatpersonen einzudringen. Dazu werden meistens Phishing-Mails verwendet. Sie täuschen eine seriöse Absicht vor und versuchen, dass der Betroffene einen Link anklickt oder einen Anhang öffnet. Aus diesem Grund sollten E-Mail-Adressen immer vor dem Öffnen überprüft werden. Als weiterer Schritt ist es wichtig, dass Firmen und Privatpersonen regelmässig Backups speichern. Dabei gilt es zu beachten, dass die externen Datenspeicher nicht am Netzwerk angeschlossen sind, sonst nützen sie nichts und sind bei einer Verschlüsselung auch betroffen.

Wie sieht die Zusammenarbeit auf nationaler und interkantonaler Ebene aus?

Die Koordination und Vernetzung erfolgt durch das schweizweite Netzwerk NEDIK (Netzwerk der Polizeibehörden zur Ermittlungsunterstützung gegen die digitale Kriminalität). Dieses soll den Austausch zwischen den Polizeikörpern beschleunigen und damit den Kampf gegen Kriminelle im Internet effizienter machen.

Was kommt im Bereich Cyberkriminalität noch auf uns zu?

Altbekannte Delikte nehmen tendenziell ab. Die Delikte verschieben sich in rasantem Tempo in Richtung virtuelle Welt. Im Internet ist es einfacher, zu Geld zu kommen, ohne gross Spuren zu hinterlassen. Um dem entgegenzuwirken, wird der Fachbereich Cyberkriminalität im Kanton Schwyz Anfang 2022 um 200 Stellenprozent verstärkt. ◇

Beliebter Gaumenschmaus: Der auf dem Waldboden stehende *Boletus edulis* zieht Pilzkenner besonders an. Auch weniger kundige Esser kennen ihn, allerdings als Fichtensteinpilz.

