Das digitale Schlachtfeld

Willkommen im virtuellen Wilden Westen: Neben Trickbetrügern und anderen Gaunern tummeln sich im Internet mittlerweile auch Hackergruppen, die von Unternehmen oder Staaten toleriert oder sogar unterstützt werden.

VON DAVID HOFER

SÜDTIROL Doch wie schafft man es, in dieser „gefährlichen" digitalen Welt sicher zu agieren? Die „Zett" hat bei Experten nachgefragt und verschiedene Aspekte genauer unter die Lupe genommen.

Cyber-Kriminalität als Milliardengeschäft

Vorsicht ist besser als Nachsicht – diese Binsenweisheit gilt auch für den digitalen Raum. Die Corona-Pandemie und die damit zusammenhängende schneller voranschreitende Digitalisierung habe zu einem deutlichen Anstieg von Cyber-Kriminalität geführt, betont Raphael Vallazza, CEO des Unternehmens Endian, das sich auf Cyber-Security spezialisiert hat: „Die Büroumgebung hat sich verändert, Homeoffice gehört nun zum Arbeitsalltag. Das bedeutet auch, dass neue Verbindungen von Zuhause ins Unternehmensnetzwerk geschaffen werden müssen. Damit ist zugleich auch die Angriffsfläche für Cyber-Angriffe größer geworden." Besonders wichtig sei es deshalb, sich gegen den Ansturm von Online-Betrügern und Hackern zu wappnen. Hier sind laut dem Experten einige Aspekte zu beachten: „Es braucht einerseits geeignete Instrumente, um sich zu schützen. Dazu gehören etwa eine Firewall oder VPN-Lösungen, um die Daten zu verschlüsseln. Außerdem ist eine Anti-Virus-Software sehr wichtig. Aber auch der Faktor Mensch spielt eine zentrale Rolle. Wer nicht sichere Passwörter verwendet oder auf Phishing-Mails eingeht, der öffnet den Kriminellen Tür und Tor."

Im Bereich der Cyber-Kriminalität habe man zuletzt eine Veränderung wahrnehmen können, mahnt Vallazza. Hackergruppen versuchen, an sensible Daten von staatlichen Einrichtungen zu kommen. Zusätzlich sei ein Anstieg von Ransomware-Angriffen zu bemerken. Dabei verschlüsseln die Kriminellen Daten und verlangen von ihren Opfern „Lösegeld". Auch Identitäten würden immer öfters geklaut, um damit falsche Rechnungen auszustellen oder sonstigen Schaden zu verursachen. Es werde immer dreister. „Organisierte Kriminalität und Hacker-Angriffe werden in Zukunft ein noch bedeutenderes Thema werden", befürchtet Vallazza. Es sei bereits jetzt ein exponentielles Wachstum festzustellen. Schließlich biete das Internet für Kriminelle eine Reihe von Annehmlichkeiten: „Wir sprechen hier von einem Milliardengeschäft. Es ist einfacher, jemanden am anderen Ende der Welt online auszurauben. Durch die Zunahme der Digitalisierung nimmt automatisch auch die Online-Kriminalität zu. Es werden immer jene Opfer ausgesucht, die am schlechtesten geschützt sind." Umso wichtiger sei es deshalb, dass sich die Menschen der Internet-Gefahren bewusst würden und lernten, sich so gut wie möglich davor zu schützen, meint Vallazza.

Der Mensch als schwächstes Glied in der Kette

Durch die auch in Südtirol immer intensiver voranschreitende Digitalisierung komme der Sicherheit im Netz eine noch fundamentalere Rolle zu, betont auch Francesco Terracciano von der Informatik AG Südtirol. Die Sensibilisierung sei durch die Corona-Pandemie noch dringender geworden, mahnt Terracciano. Die Spielarten der Cyber-Kriminalität hätten sich verändert, die Verwendung von sensiblen Gesundheitsdaten biete eine neue Angriffsfläche: „Sensible Personendaten, insbesondere aus dem Gesundheitsbereich, haben auf Hacker immer eine besondere Anziehungskraft. Im Dark Web etwa kann man Krankenakten um einige Dollar erwerben, das macht die Sache für Kriminelle lukrativ." Diese Entwicklung ist eine Herausforderung für alle, die mit der Abwehr von Cyber-Attacken zu tun haben, auch staatliche Einrichtungen und Sicherheits-Agenturen. Vonseiten des Außenministeriums sei etwa zu hören, dass seit Beginn der Krise ein enormer Anstieg von Online-Attacken zu bemerken ist. Die Informatik AG habe in den vergangenen Jahren sehr viel an Erfahrung gewonnen und könne nun auf die Bedrohungen reagieren, sagt Terracciano. Dazu würden die Risiken auf europäischer Ebene immer wieder gezielt analysiert. So können schon präventiv Maßnahmen getroffen werden.

Damit ein guter Schutz gewährleistet ist, bedarf es laut Terracciano aber eines speziellen Faktors: „Das schwächste Glied in der Kette ist der Faktor Mensch. Häufig fehlt es hier am nötigen Risikobewusstsein, was dazu führt, dass Hacker und Betrüger leichtes Spiel haben. Sich über Risiken zu informieren und sich ihrer bewusst zu sein, ist deshalb für jeden Menschen, der sich in der digitalen Welt aufhält, essenziell. Jede und jeder von uns kann hier mehr tun!"

Sich seiner Gegner bewusst werden

„Spionagetätigkeiten von staatlichen Stellen haben längst auch den digitalen Raum erreicht", betont Edgar Weippl von der Fakultät für Informatik der Uni Wien. So waren die Enthüllungen von Edward Snowden rund um die NSA für ihn auch nicht verwunderlich – schließlich würden Geheimdienste genau dafür geschaffen. Allerdings sei die technische Ausführung sicherlich faszinierend. Neben diesen „offiziellen Spionagetätigkeiten" gebe es allerdings noch eine ganze Reihe von anderen Organisationen, die sich im World Wide Web tummeln. Dazu gehören etwa auch Hackergruppen, die zwar nicht im Auftrag von gewissen Staaten agieren, aber von ihnen toleriert oder gar unterstützt würden: „Ein Beispiel ist hier etwa der Ukraine-Konflikt, in dem auf der einen Seite russlandfreundliche Gruppen Stellen in der Ukraine hacken. Auf der anderen Seite gibt es aber auch ukrainefreundliche Gruppen, die versuchen, russische Stellen anzugreifen." Vor allem Russland und China werden immer wieder mit derartigen Aktivitäten in Verbindung gebracht, tatsächlich dürfte das Phänomen aber deutlich weiterverbreitet sein.

Bei vielen Hackergruppen seien allerdings politische oder gar ideologische Motive nicht der entscheidende Anreiz. Vielmehr gehe es um den finanziellen Aspekt. Dafür würden vor allem Datenbanken großer Unternehmen ins Visier genommen, mit dem Ziel, eine Art Lösegeld dafür zu erhalten. Hier habe sich mittlerweile sogar eine Art Arbeitsteilung gebildet: „Da gibt es verschiedene Stellen, die sich jeweils auf nur einen bestimmten Aspekt des Angriffs konzentrieren." Diese Art der Kriminalität werde wohl noch weiter ansteigen, befürchtet Weippl – nicht zuletzt, da aufgrund der Krise die Digitalisierung schneller, hektischer vonstatten gehen musste, als noch in den Jahren zuvor der Fall gewesen sei.

Der Schutz gegen solche Angriffe ist keine leichte Angelegenheit, weder für Staaten, noch für Unternehmen oder Privatpersonen. Während Staaten und Unternehmen auf weitaus mehr Ressourcen zurückgreifen können, seien für Privatpersonen vor allem drei Überlegungen wichtig: „Als erstes muss ich mich fragen, welche Daten ich habe und wie wichtig deren jeweiliger Schutz für mich ist. Dann muss ich mir ein realistisches Bild meiner Gegner vor Augen führen. Also die Frage stellen, vor wem muss ich mich realistischerweise in Acht nehmen." Für Privatpersonen seien etwa Geheimdienste im Regelfall keine realistischen Gegenspieler – organisierte Online-Betrüger aber schon, betont der Experte. Anschließend gelte es, sich darüber zu informieren, welche Schutzmöglichkeiten man hat. Das reiche von speziellen Programmen, über externe Festplatten bis hin zu effektivem Passwortmanagement.

Hässliches Passwort? Gute Wahl!

SÜDTIROL *(dah)* Ivo Plotegher, stellvertretender Kommissar der Staatspolizei und Leiter der Post- und Kommunikationspolizei in Bozen, im Interview über Grundregeln im Netz und Merkmale eines sicheren Passworts.

Z Herr Plotegher, welche Verhaltensregeln sollte man im Zusammenhang mit Betrügereien und Straftaten im Internet beachten?

Ivo Plotegher: Im Laufe der Jahre habe ich beobachtet, dass die Menschen im Netz allgemein weniger vorsichtig sind als im Alltag. Deshalb kann es vergleichsweise leicht passieren, im Netz zum Opfer zu werden. Wenn man sich online aber so vorsichtig wie im täglichen Leben verhält, kann man so manche unangenehme Überraschung vermeiden.

Z Wird die Kriminalität im digitalen Raum in Zukunft zunehmen?

Was Straftaten im Netz anbelangt, ist die aktuelle Lage nicht alarmierend. Dies ist auch ein Ergebnis der seit Jahren geleisteten Sensibilisierungsarbeit der Polizeidienststelle für Post und Kommunikationswesen und anderer Behörden. Es ist jedoch klar, dass eine ganze Reihe von kriminellen Tricks ihren Weg von der „realen Welt" ins Internet gefunden haben.

Z Was ist für eine Privatperson bei im Internet absolut tabu?

All jene Dinge, die man auch im täglichen Leben vermeiden würde. Zum Beispiel sollte man auf keinen Fall – auch nicht der Person, der man am meisten vertraut – Fotos schicken, auf denen man in unangebrachten Posen oder unbekleidet zu sehen ist. So kann vermieden werden, dass man zum Opfer von „Revenge Porn", „Sextortion" oder Cybermobbing wird. Fotos von Kindern und Jugendlichen könnten zudem das Interesse von Pädophilen wecken.

Z Abschließend gefragt: Was zeichnet ein sicheres Passwort aus?

Das Passwort muss aus mindestens acht Zeichen bestehen. Zudem sollten sowohl Sonderzeichen, Ziffern, als auch Groß- und Kleinbuchstaben enthalten sein. Man könnte zusammenfassend sagen, dass ein „hässliches Passwort" ein gutes Passwort ist.