Abo Erfahrungsberichte und Livedemonstrationen

Wie Hacker Schwachstellen nutzen können

Der Datenschutztag gab Einblick in die Welt der Hacker und Cyberkriminalität.

05. Februar 2026, 21:56 Uhr 06. Februar 2026, 10:00 Uhr

Sina Thöny

Artikel anhören

Je mehr man sich informiere, desto besser könne man sich schützen, meinten die Redner am gestrigen Datenschutztag. (Bild: Daniel Schwendener

Über 88 000 Anmeldungen seien für den diesjährigen Datenschutztag eingegangen. «Ich bin enttäuscht, dass nur so wenige von ihnen erschienen sind», meinte Marie-Louise Gächter, Leiterin der Datenschutzstelle, zum fast voll besetzten Triesner Saal. Doch mit dem Erscheinen so vieler Interessierter hatte sie nicht wirklich gerechnet. Denn ironischerweise wurde das Anmeldetool des Datenschutztags gehackt. Zahllose Anmeldungen liefen über die E-Mail-Adresse ilovehacking@xy.li, mit denen sich eine Täterschaft einer Schwachstelle des Systems bediente und sich einen Scherz erlaubte. Leicht ärgerlich für den Veranstalter, doch ein guter Einstieg in den Abend, der sich ganz der Welt der Hacker und der Cyberkriminalität widmete.

Thermostat bis zum USB-C-Kabel

Auf die erste unfreiwillige und wohl ungeplante Livedemonstrationen folgte der Einblick in den Alltag eines professionellen «Hackers»: Cybersicherheitsexperte Sebastian Schreiber prüft mit seinem Unternehmen die Sicherheit verschiedener Geräte oder anderer digitaler Anwendungen. Dabei gehen er und seine Mitarbeitenden vor wie echte Hacker. Sie suchen nach Schwachstellen im System und nutzen diese, um an Daten zu gelangen oder um die Geräte zu missbrauchen. Dass es sich hierbei nicht immer um grosse Fische wie Server oder Überwachungssysteme handeln muss, zeigt Schreiber am Beispiel eines Thermostats. Wieso dieses Ziel eines Angriffes werde könnte, scheint auf den ersten Blick fraglich. Doch Schreiber erklärte: «Hiermit kann die Temperatur von Rechenzentren oder Kraftwerken gesteuert werden.» Temperaturschwankungen können in diesen empfindlichen Systemen verheerende Folgen haben. Dennoch ist das Hacken eines solchen Thermostats eine Sache von wenigen Sekunden – natürlich nur mit etwas Vorarbeit und der richtigen Software. Und schon konnte Schreiber per Funkwellen das Thermostat ganz einfach von seinem Computer aus steuern.

Sebastian Schneider zeigte live, wie schnell man einen Thermostat hacken kann. (Bild: Daniel Schwendener)

Ein anderes Beispiel und eine Gefahr, die viele unterschätzen, betrifft die Smartphones: Ein frisch aufgenommenes Foto soll von einem Handy auf ein anderes übertragen werden, ohne dass der Hacker das Handy seines Opfers in die Hand nehmen muss. Dafür brauchte Schreiber nur ein unscheinbares USB-C-Kabel, welches er mit einem kleinen Chip versehen hatte. Von aussen liess sich das Kabel aber nicht von anderen seiner Art unterscheiden. Kaum war das Handy eingesteckt, surrt schon das andere Handy und das Foto ist übertragen. Ein Trick, der auch von den ganz Grossen genutzt wird: «Die NSA hat bei ihren Spionagen genau das Gleiche gemacht», so Schreiber. Auch USB-Sticks mit Zahlen- oder Fingerabdruckschloss sind für den Experten kein Hindernis. Zum Staunen der Menge verschickte er SMS unter falschen Nummern oder änderte mit wenigen Anpassungen an der URL den Preis eines Buches in einem Onlineshop. Sein Ziel ist es, auf Sicherheitslücken hinzuweisen: «Wir finden die Lücken, damit die Verantwortlichen sie schliessen können.»

Zum Inhalt springen

Hacker testen das System auf Schwachstellen und nutzen diese aus, so Schneider. (Bild: Daniel Schwendener)

«Protect your system, amigo»

Was passieren kann, wenn solche Sicherheitslücken ausgenutzt werden, erzählte Martin Häring, Leiter Compliance der Universität Liechtenstein. Als die Universität rund vier Jahren Opfer eines Ransomware-Angriffes wurde, feierte Häring auf den Tag genau sein einjähriges Arbeitsjubiläum bei der Universität: «Ich war noch komplett grün hinter den Ohren.» Der Schock sass tief, als am Morgen des 16. August alle technischen Systeme, E-Mails, WLAN und Weiteres ausfielen. Auf dem Server fanden sie die Botschaft der Angreifer: Alle Daten wurden verschlüsselt. Wenn die Universität sie zurück will, muss sie ein Lösegeld zahlen. Auch einen Ratschlag, was man nun dem Chef sagen sollte, hatten die Hacker parat: «Protect your system, amigo», hiess es in der Botschaft.

um Inhalt springen

Martin Häring berichtete vom Ransomeware-Angriff auf die Universität Liechtenstein. (Bild: Daniel Schwendener)

Die nächsten Tage floss der Kaffee in der IT-Abteilung in Strömen, erzählte Häring. Zuerst wurden alle wichtigen Stellen informiert und die Universität konnte sich auch Hilfe von Experten aus Belgien holen. Zum Glück konnte die Universität auf Back-ups zurückgreifen. «Wir entschieden uns, nicht zu zahlen», so Häring. Doch mit den Hackern verhandelten sie trotzdem – grösstenteils zum Zeitschinden, aber auch aus Neugier, wie viel sie verlangen würden. Umgerechnet 900 000 Franken wollten die Hacker für die Daten. Auch mit einem angebotenen Rabatt von 30 Prozent ging die Universität nicht auf den Deal ein.

> Man sollte faktisch die Risiken analysieren und für sich abwägen, wie man mit ihnen umgeht.

«Wichtig ist es, sich über solche Risiken zu informieren», meinte Gächter in der anschliessenden Diskussion. Schreiber und Häring stimmten zu: «Man sollte faktisch die Risiken analysieren und für sich abwägen, wie man mit ihnen umgeht», so Schreiber. Denn zahllose Risiken und Schwachstellen verbergen sich. Doch je besser man sie kennt, desto eher kann man sie umgehen.