Basel Stadt Land Region

Die perfiden Maschen der Internet-Täter

Cyber-Attacke auf Uni Basel Betrüger haben bei mehreren Schweizer Hochschulen Lohnzahlungen abgezweigt. Die wichtigsten Fragen und Antworten rund um Betrug und Erpressung im Internet und Tipps zum eigenen Schutz.

Nina Jecker

Ob Betrug oder Erpressung: Kriminelle gehen im Internet immer gezielter vor, um ahnungslose Opfer zu täuschen. Foto: VQH

— Wie konnten die Täter das Sicherheitssystem der Uni austricksen?
Am Wochenende wurde bekannt, dass unter anderem die Universität Basel Opfer einer Internet-Attacke geworden ist. Hacker haben sich laut der «Sonntags-Zeitung» offenbar durch sogenannte Phishing-E-Mails, bei denen Login-Daten erschlichen werden, Zugang zu den Systemen mehrerer Hochschulen verschafft. Dort änderten sie dann die Empfängerkonten für Lohnzahlungen und wiesen sich das Geld selber zu. Uni-Sprecher Matthias Geering hat der BaZ einen Screenshot des verwendeten Phishing-Mails gezeigt. Die Nachricht, die an Uni-Angestellte verschickt wurde, ist als internes E-Mail kaschiert. Der Trick: Den Empfängern wird mitgeteilt, sie hätten eine neue Sprachnachricht erhalten. Nach dem Klick auf den Link erscheint dann eine Webseite zum Login, die ebenfalls im Design der Universität aufgezogen wurde.

Auch andere Hochschulen sind betroffen, wie viele genau, ist derzeit unklar. Die gesamte Deliktsumme liegt laut der Staatsanwaltschaft Basel-Stadt im sechsstelligen Bereich; der Uni Basel ist ein Schaden von rund 15'000 Franken entstanden. Die Universität Zürich gab an, ebenfalls verdächtige Angriffe verzeichnet zu haben, die aber rechtzeitig erkannt worden seien.

— Wo haben Täter vor kurzem ebenfalls zugeschlagen?
Auch der Fall Stadler Rail hat dieses Jahr für Schlagzeilen gesorgt. Am 7. Mai gab das Unternehmen mit Sitz im Kanton Thurgau bekannt, dass es Kriminellen gelungen sei, ins IT-System einzudringen und Daten zu stehlen. Um die Datensätze zurückzuerhalten, sollte das Unternehmen sechs Millionen Dollar in der Kryptowährung Bitcoin bezahlen. Die Erpresser veröffentlichten Daten im Darknet, um Druck aufzubauen. Stadler-Patron Peter Spuhler verweigerte jedoch jegliche Zahlung und erstattete Anzeige. Das Unternehmen habe von allen gestohlenen Daten funktionierende Sicherungskopien, liess Stadler verlauten. In einem aktuellen Fall hat sich ein Unternehmen aus dem Raum Liestal anders entschieden. Hacker hatten der Technikfirma über eine Schadsoftware sämtliche Daten verschlüsselt und ein Lösegeld in sechsstelliger Höhe verlangt. Da in diesem Fall Sicherungskopien fehlten, entschied sich der Inhaber schliesslich, auf die Forderungen einzugehen, worauf ihm die Erpresser einen Teil der benötigten Daten wieder zur Verfügung stellten.

Die Staatsanwaltschaft Basel-Stadt geht davon aus, dass einige Firmen keine Anzeige erstatten, um die eigene Reputation nicht zu gefährden.

— Wie verschaffen sich die Kriminellen Zugang zu den Systemen?
In ein gesichertes System kann man auf verschiedene Arten eindringen. Zum einen über Phishing-E-Mails, in denen unter Vorwänden Zugangsdaten verlangt werden. Diese Masche wird auch bei Privatpersonen angewendet, um an Bank- und Kreditkartendaten zu kommen. Die Täter passen dabei ihre Nachrichten dem Corporate Design der entsprechenden Firma an.

Fälschungen sind auf den ersten Blick meist nicht erkennbar.

Eine zweite Möglichkeit ist das Installieren von Schadsoftware. Dazu gehört die sogenannte Ransomware, mit der Daten verschlüsselt und Rechner blockiert werden können, bis ein Lösegeld bezahlt wird. Die Installation geschieht in den meisten Fällen über E-Mails, in denen auf einen Link geklickt werden muss. Aber auch Programme zum Download und Links auf Webseiten können Ransomware enthalten. Ein PC kann sogar infiziert werden, wenn man damit nur auf einer infizierten Webseite surft. Ist ein PC einer Firma betroffen, kann sich die Software auch auf das ganze Firmensystem ausbreiten.

— Welche Maschen wenden Kriminelle bei Privatpersonen an?
Neben den Phishing-Mails gibt es zahlreiche weitere Betrugsvarianten. Dazu gehört unter anderem der Love-Scam, bei dem Opfern im Internet die Existenz eines Traumpartners vorgegaukelt wird. Irgendwann wird der oder die «Liebste» dann mit einer Lüge um Geld bitten.

Die Sextortion genannte Erpressung zielt bei persönlichen Kontakten im Internet darauf ab, andere dazu zu bringen, vor dem PC zu masturbieren. Häufig, indem sich das Gegenüber zuerst ebenfalls freizügig zeigt. Danach werden die meist männlichen Opfer mit den Bildern erpresst.

Andere geben nur vor, kompromittierendes Material zu besitzen. Dafür werden E-Mail-Adressen und Passwörter von Kunden beispielsweise von Online-Versandhäusern ergaunert. Diese Kunden schreiben die Hacker dann an und behaupten, sie hätten sich Zugriff auf deren PC verschaffen und sie beim Pornokonsum filmen können. Auch hier wird häufig ein Lösegeld verlangt.

Zu den ältesten Tricks gehören wahllos verschickte E-Mails, in denen ein Lotteriegewinn oder eine Erbschaft in Aussicht gestellt werden. Um an die versprochenen Summen zu kommen, muss der Empfänger aber vorgängig selber eine Überweisung tätigen. Den Geldsegen erhält er selbstverständlich nie.

Auch Handys sind nicht sicher. Betrüger haben vor wenigen Tagen versucht, über SMS-Nachrichten, die angeblich von der Eidgenössischen Steuerverwaltung stammen, Empfänger zum Klick auf einen Link zu animieren. Von der Post ist ausserdem eine gefälschte App im Umlauf.

Weitere Informationen und aktuelle Warnhinweise zu den neuesten Tricks bietet die Kantonspolizei Basel-Stadt online.

— Wie kann man sich schützen?
Es ist gar nicht so einfach, sich vor Cyberangriffen zu schützen. Sobald eine Masche nicht mehr funktioniert, erproben die Täter neue. Ausserdem sind Fälschungen auf den ersten Blick meist nicht erkennbar. Wie im Beispiel der Uni Basel werden ganze Webseiten nachgebaut, um die Opfer zu täuschen.

Die Polizei rät deshalb, nie auf Links von Nachrichten zu klicken, die unerwartet kommen. Ausserdem soll man nirgendwo seine Kreditkarten- oder Kontodaten angeben. Hilfreich kann auch der Blick auf den Absender sein. Häufig ist das E-Mail zwar täuschend echt, aber die Adresse hat mit der angegebenen Firma nichts zu tun.

Grundsätzlich sollte man mit seinen Daten, aber auch mit anderen intimen und persönlichen Handlungen und Dingen wie Fotos oder Videos im Internet mindestens genauso vorsichtig umgehen wie in der realen Welt.

Die Schutzsoftware eines Computers sollte immer aktuell gehalten werden. Ausserdem wird Firmen geraten, die Mitarbeitenden für die Gefahren zu sensibilisieren. Wer unverzichtbare Daten hat, sollte unbedingt laufend Sicherungskopien erstellen, um im Fall eines Ransomware-Angriffs nicht erpressbar zu sein.

— Was tun, wenn man bereits Opfer geworden ist?
Opfer sollen sich an die Strafverfolgungsbehörden wenden. Die Schweizerische Kriminalprävention rät davon ab, auf Erpressungsversuche einzugehen, da es keinerlei Sicherheit gibt, dass die Täter bei Bezahlung des die Daten tatsächlich wieder zur Verfügung stellen. In seltenen Fällen gelingt es Experten, verschlüsselte Daten zu entschlüsseln.

— Wer sind die Täter und wie können sie geschnappt werden?
Man weiss, dass viele Love-Scams und andere Betrugsmaschen von der Elfenbeinküste aus organisiert werden. In grösseren Fällen führten Spuren auch nach Russland. Oft bleibt es aber komplett im Dunkeln, wo sich die Täter aufhalten. Sie kommen in der Regel straflos davon, da sie fast immer aus dem Ausland agieren und ihre Spuren gut verwischen. Eine Rückverfolgung sei mit grossem Aufwand verbunden, sagt Toprak Yerguz, Sprecher der Kantonspolizei Basel-Stadt.