Informationssicherheit und eHealth

Identitätsmissbrauch im Internet

eHealth Aktuell

Reinhold Sojer

Dr., Wissenschaftlicher Mitarbeiter FMH eHealth

Beim Identitätsdiebstahl werden personenbezogene Daten missbräuchlich durch kriminelle Dritte entwendet und genutzt, um sich entweder finanziell zu bereichern oder um das Opfer gezielt zu schädigen. Da die Identität etwas ist, was im eigentlichen Sinne nicht gestohlen werden kann, wird richtigerweise der Begriff Identitätsmissbrauch verwendet. Dieser Begriff soll erstmals mit der Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz im Kontext des Ausbaus der strafrechtlichen Sanktionen im Schweizer Strafrecht aufgenommen werden.

Der Identitätsmissbrauch wird immer in zwei Schritten durchgeführt:

1. Zuerst erfolgt der Diebstahl von persönlichen Informationen,
2. danach werden die gestohlenen Informationen benutzt, um einen Missbrauch oder Betrug zu begehen.

Die persönlichen Informationen, die eine Person in der digitalen Welt identifizieren, werden durch Angreifer entweder ausgespäht oder durch Angriffe auf Kontendaten von Anbietern der Onlinedienste erbeutet. Für den Identitätsmissbrauch genügen bereits wenige Informationen wie Name, Adresse oder Geburtsdatum. Solche persönlichen Daten werden häufig bei der Registrierung von Onlinediensten, insbesondere Social Media, verlangt oder als Sicherheitsmerkmal bei telefonischen Verträgen zur Verifikation der Identität des Anrufers erfragt.

Für den Identitätsmissbrauch genügen bereits wenige Informationen wie Name, Adresse oder Geburtsdatum.

In welchem Ausmass Angreifer Daten erbeuten können, zeigt der Fall des Internetkonzerns Yahoo: Im August 2013 meldete Yahoo den Vorfall eines Cyber-Angriffs. 2017 wurde bekannt, dass bei diesem Angriff persönliche Informationen von mehr als 3 Milliarden Konten gestohlen wurden. Die Angreifer erhielten Zugang zu Daten wie Namen, E-Mail-Adressen oder Telefonnummern, die für weitere Angriffe von Interesse sind und die gezielt für einen Identitätsmissbrauch verwendet werden können.

Mit solchen gestohlenen Informationen werden im Namen des Opfers Waren bestellt oder falsche Informationen verbreitet, mit dem Ziel der Rufschädigung oder des Mobbings. Besonders beachtenswert ist der Anstieg der Entwendung von Gesundheitsdaten gemäss dem *Breach Level Index* (breachlevelindex.com), einer weltweiten Datenbank zur Registrierung von Datensicherheits- und Datenschutzverletzungen. Im Jahr 2015 wurde der zweitgrösste Krankenversicherer in den USA Anthem Opfer eines Cyber-Angriffes, bei dem Daten von 78 Millionen Versicherten gestohlen wurden. Auch wenn keine medizinischen Daten direkt betroffen waren, so liegt das Schadenspotential im Versicherungsbetrug oder in der Erpressung anhand persönlicher Informationen. Das höchste Schadenspotential entsteht jedoch dann, wenn Angreifer zusätzlich in Kenntnis von Passwörtern gelangen.

Phishing = Password + Harvesting + Fishing

Um an geheime Informationen zu gelangen, werden Methoden des *Social Engineering* eingesetzt, welche darauf abzielen, die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen auszunutzen. Eine häufige Methode zum Erspähen von Passwörtern ist *Phishing*. Phishing ist ein Kunstwort aus Password, Harvesting und Fishing und täuscht eine Person mit gefälschten E-Mails, Websites oder Twitternachrichten, um in den Besitz von persönlichen Login-Daten zu gelangen. Als Absender wird eine namhafte Organisation oder im Fall eines finanziellen Betruges eine Bank angegeben. Aber auch Schadprogramme können dazu verwendet werden, um eine Person auf eine böswillige Website zu führen (z.B. durch Browser-Hijacker). Hat es der Phisher auf Zugangsdaten für Onlinedienste abgesehen, sendet er ein Spam-E-Mail ungezielt an möglichst viele Empfänger und spekuliert darauf, dass unter den vielen Empfängern auch Kunden des ent-

sprechenden Onlinedienstes, auf die er es abgesehen hat, reagieren. Effizienter ist das Versenden von betrügerischen E-Mails unter Verwendung gekaufter oder gehackter Adressen wie im Fall des Internetkonzerns Yahoo. Der Empfänger wird nun im nächsten Schritt innerhalb der gefälschten Website aufgefordert, sich mit seinem Benutzernamen und seinem Passwort auszuweisen, und somit gelangen diese Daten in die Hände der Cyber-Kriminellen. Seit einigen Jahren werden Phishing-Angriffe auch mit *Ransomware*-Schadsoftware kombiniert (siehe SÄZ 2016;97(49–50):1708–9). Eine Sonderform des Phishings ist das sogenannte Spear-Phishing, bei dem der Angreifer nicht nur die E-Mail-Adresse des Opfers kennt, sondern auch Details aus dem privaten und beruflichen Umfeld. So kann der Angreifer im Namen einer vertrauenswürdigen Person oder Organisation mit einer plausiblen Aufforderung etwa per E-Mail oder über Facebook dazu bewegen, eine bestimmte Aktion auszuführen. Mit diesem Vorgehen wurden im Sommer 2016 in Deutschland gezielt Nachrichten mit dem gefälschten Absender hq.nato.int an Politiker versendet, welche Informationen zum Militärputsch in der Türkei enthielten und unter anderem auch einen Link zu einer mit Schadcode infizierten Website.

Anwendungen wie Twitter, WhatsApp, Facebook, Instagram oder Google Translate sammeln unentwegt persönliche Informationen.

Je mehr persönliche Daten über das Opfer ausgespäht werden können, desto authentischer kann die betrügerische Nachricht gestaltet werden. Anwendungen wie Twitter, WhatsApp, Facebook, Instagram oder Google Translate sammeln unentwegt persönliche Informationen, haben Zugriff auf Kontaktdaten, Kalender oder den Standort und: Sie wissen am besten, wer Sie sind.

Wie kann man sich schützen?

Gegen einen Identitätsmissbrauch gibt es keinen hundertprozentigen Schutz. Dies liegt einerseits daran, dass persönliche Daten in diversen Institutionen (Banken, Versicherungen, Spitäler usw.) gespeichert werden und auf diese nur noch wenig Einfluss genommen werden kann. Andererseits gehen Cyber-Kriminelle bei der Beschaffung von Identitäten meist professionell vor, und die in diesem Artikel benannten Methoden stellen nur ein kleines Spektrum derer dar, die heute genutzt werden. Auch werden sie kombiniert angewendet mit Methoden jenseits der digitalen Welt, wie zum Beispiel dem *Dumpster Diving* (Durchsuchen von Abfällen nach persönlichen Informationen).

- Machen Sie sich mit der Thematik Identitätsmissbrauch vertraut und setzen Sie sich damit auseinander. Die richtige Awareness schützt bereits nachhaltig.
- Schützen Sie sich vor Schadsoftware (Malware), indem Sie Ihre Systeme stets auf den neusten Stand halten und Sicherheitsupdates umgehend installieren (siehe Empfehlungen aus SÄZ 2016;97(49–50): 1708–9).
- Geben Sie personenbezogene Daten äusserst «sparsam» und nur auf vertrauenswürdigen Websites und Portalen ein. Verwenden Sie nie Ihr reales Geburtsdatum in sozialen Netzwerken.
- Misstrauen Sie E-Mails, die Sie unaufgefordert bekommen, und seien Sie vorsichtig, wenn Sie E-Mails erhalten, die eine Aktion von Ihnen verlangen und andernfalls mit Konsequenzen drohen.
- Öffentliche WLANs bergen die Gefahr des Abhörens durch Dritte. Wenn Sie sensitive Informationen austauschen, sollten Sie diese durch Nutzung einer zusätzlichen Verschlüsselungsebene (HTTPS, VPN oder spezielle Browser-PlugIns) schützen.
- Verwenden Sie keinesfalls stets die gleichen Passwörter für verschiedene Internetkonten und ändern Sie diese von Zeit zu Zeit. Die Verwendung verschiedener Benutzernamen für Onlinedienste erschwert Betrügern, ein Gesamtprofil Ihrer Identität zu erstellen.

Gegen einen Identitätsmissbrauch gibt es keinen hundertprozentigen Schutz.

- Nutzen Sie wo immer möglich die Zwei-Faktor-Authentifizierung (2FA). Bei der 2FA wird unter anderem neben Benutzername und Passwort ein Nachweis in Form eines Besitzes verlangt. Dies kann eine TAN-Liste oder ein Security Token wie eine Smartcard sein, welche ausschliesslich im Besitz des Kontoinhabers ist.
- Verwenden Sie eine adäquate Endpoint-Security-Software (Virenscanner, Firewall usw.) und halten Sie diese aktuell.

Recherchieren Sie proaktiv im Internet, welche Daten von Ihnen gespeichert sind, und überprüfen Sie, ob diese korrekt sind. Unter der Adresse https://haveibeenpwned.com können Sie überprüfen, ob Ihre E-Mail-Adresse oder Benutzerkonto kompromittiert wurde.

Korrespondenz:
Dr. rer. biol. hum.
Reinhold Sojer
Wissenschaftlicher Mitarbeiter / Stv. Leiter Abteilung Digitalisierung / eHealth
FMH Verbindung der Schweizer Ärztinnen und Ärzte
Elfenstrasse 18
Postfach 300
3000 Bern 15
Telefon: +41 31 359 12 04
reinhold.sojer[at]fmh.ch