Die vernetzte Gesellschaft – ein Eldorado für Cyberkriminelle

Die zunehmende Akzeptanz von Onlineangeboten führt in der Internetökonomie zu sogenannten positiven Netzeffekten. Alle Akteure profitieren und ziehen weitere Teilnehmer nach. Dazu gehören aber auch Cyberkriminielle, die Privatpersonen wie Firmen gleichermassen massiv schädigen können. Oliver Kamin

Internetgestützte Angebote und soziale Medien halten in unserer vernetzten Gesellschaft nicht nur im Privatleben, sondern auch in Firmen vermehrt Einzug. So sind aus vielen Unternehmensbereichen wie Marketing, Vertrieb, Öffentlichkeitsarbeit oder Kundenbeziehungsmanagement soziale Medien kaum mehr wegzudenken. Sie werden besonders dann wichtig, wenn sich Unternehmen als modern, kundennah und innovativ darstellen wollen. Aber auch beim privaten und geschäftlichen Informationsaustausch hat sich mit den Jahren das Kommunikationsverhalten verändert. Weg vom klassischen Brief respektive analogen Festnetztelefon kommunizieren Personen beruflich und privat immer häufiger auf digitalem Weg via SMS, E-Mail und in den letzten Jahren auch über Internetdienste wie Voice over IP, Chat oder soziale Plattformen.

Eine solch zunehmende Akzeptanz von Onlineangeboten führt in der Internetökonomie zu sogenannten positiven Netzeffekten. Hiermit ist gemeint, dass das Wachsen eines Netzes beziehungsweise eines netzgestützten Angebots (auch Netzwerkgut genannt) den Nutzen für die Akteure (Anbieter und Anwender) steigert und nahezu automatisch weitere Teilnehmer anzieht. Im Idealfall sind dies dann weitere Anwender, die das Netzwerkgut nutzen möchten, oder weitere Anbieter, die beabsichtigen, das Netz mit eigenen Produkten weiter anzureichern. Im negativen Sinne werden aber auch Cyberkriminelle stärker motiviert, in solchen Netzen zu agieren, um ihre Motive durch illegale Handlungen in sozialen Netzen respektive Medien bestmöglich zu verfolgen.

Dr. Oliver Kamin ist Studiengangsleiter für Wirtschaftsinformatik und Business-/IT-Consulting an der Fernfachhochschule Schweiz.

Cyberkriminelle profitieren über Social Engineering von der Unbedarftheit vieler Onlinenutzer. Bild: Fotolia

Wie gehen Cyberkriminelle vor?

Durch die Omnipräsenz und die Etablierung sozialer Netze werden die Gefahren oft unterschätzt oder erst gar nicht gesehen. Hierbei soll es nicht nur um den Datenschutz gehen, wenn beispielsweise Angebote (in der Regel soziale Plattformen oder Dienste) mit Sitz im Ausland genutzt werden, sondern auch um die in den letzten Jahren stark anwachsende Cyberkriminalität. Diese kann in Form von Identitätsdiebstahl oder Social Engineering auftreten. Hieraus ergeben sich neue und andersartige Sicherheitsrisiken sowohl für Personen als auch für Körperschaften.

Allein ein Blick in die Medienberichterstattung der letzten Zeit zeigt, dass der Identitätsdiebstahl im Internet zugenommen hat. Hierbei ist es nicht zwingend erforderlich, dass mit grossem technischem Aufwand Benutzerkonten von Personen/Körperschaften gehackt und anschliessend gekapert werden. Identitätsdiebstahl kann mit vergleichsweise einfachen Mitteln initiiert und vollzogen werden. Viele Cyberkriminelle begnügen sich hierbei zunächst damit, die anvisierten Konten oder die zu versendenden Nachrichten schlichtweg zu fälschen, um dann durch entsprechende Interaktionen mit diesen Konten oder Nachrichten an die gewünschten Daten der anvisierten Person/Körperschaft selbst oder des direkten Umfelds zu kommen. Sowohl beim Fälschen als auch beim Kapern erfolgt der Identitätsdiebstahl in der Regel nicht auf einem einzigen Kanal. Es wird gezielt die Vernetzung mit anderen Konten des Angriffziels und den damit verbundenen weiteren Konten anderer ausgenutzt, um durch Rasterung an weitere Daten zu kommen.

Ein weiteres Problem ist, dass häufig das Kommunikationsverhalten von Privatpersonen zu offenherzig und dasjenige von Mitarbeitern in Unternehmen zu unkritisch ist. Dies begünstigt das sogenannte Social Engineering, das Cyberkriminelle praktizieren. Hierbei werden unter anderem Konten und Nachrichten von Personen und Körperschaften systematisch nach Hinweisen durchsucht, um beispielsweise Passwortfragen für eventuell andere genutzte Konten der Betroffenen (etwa für Social-Media-, Cloud-, Mail- oder Webhosting-Dienste) beantworten zu können. Hintergrund ist der, dass viele Dienstanbieter unter anderem eine Passwortfrage wie «Wie lautet der Mädchenname Ihrer Mutter?» oder die Angabe von Zahlungsverkehrsdaten als alleiniges oder mit anderen Angaben kombiniertes Authentifizierungsmittel verwenden, um vergessene Passwörter wiederherzustellen. Werden hierdurch Konten gekapert oder Identitäten gestohlen, wird das Social Engineering für den Cyberkriminellen weiter erleichtert. Sie können so vom gekaper- ▶

ten Konto (mithilfe der im Adressbuch oder der Mailkorrespondenz gefundenen Empfänger) weitere gefälschte Nachrichten versenden mit der Aufforderung, Informationen an eine bestimmte Stelle zu kommunizieren. Beim unberechtigten Zugang zu einem Webhosting- oder Cloud-Speicher kann für den Cyberkriminellen gar der vorgenannte Schritt entfallen, wenn die gesuchten persönlichen oder betriebsinternen Daten dort abgelegt sind.

Was sind die Motive von Cyberkriminellen?

Zielsetzung bei solchen Aktivitäten ist es, ein möglichst komplettes Profil der attackierten Person, Körperschaft oder des Eigners zu erhalten, um beispielsweise anschliessend in dessen Namen aufzutreten und zu agieren oder auf seine persönlichen oder internen Daten zugreifen zu können. Dies geschieht häufig, um den Eigner zu schaden, die gewonnenen Daten und Informationen im Sinne des Cyberkriminellen zu verwerten oder an weitere private oder betriebsinterne Daten des Eigners zu kommen. Die häufigsten Motive sind hierbei:

- **Namensmissbrauch:** In Blogs, Wikis oder Foren nimmt der Cyberkriminelle die Identität des Eigners an und verfasst diffamierende oder diskreditierende Beiträge.
- **Geschäfte:** Der Cyberkriminelle nimmt die Identität des Eigners an und bestellt Waren und Dienstleistungen zulasten der angegriffenen Person/Körperschaft.
- **Spionage:** Die ausgespähten Daten des Eigners (insbesondere Unternehmen oder andere Institutionen) werden an andere konkurrierende oder gegnerische Körperschaften gegen Bezahlung weitergegeben.
- **Desinformation:** Im Namen des Eigners werden Sachverhalte, die nicht der Wahrheit entsprechen oder in einem falschen Zusammenhang dargestellt werden, in Umlauf gebracht.
- **Falschverdächtigung:** Es wird mithilfe des Namens oder persönlicher respektive interner Daten des Eigners agiert, um andere Personen und Körperschaften gezielt zu verleumden, damit Falschanzeigen provoziert oder diese gar selbst durch den Cyberkriminellen aufgegeben.
- **Erpressung:** Dem Eigner wird gedroht, eine oder mehrere der oben aufgeführten Handlungen zu vollziehen, wenn keine Geldzahlungen an den Cyberkriminellen geleistet oder andere Bedingungen erfüllt werden.

Hat ein Cyberkrimineller Erfolg, ist es zu erwarten, dass er zulasten des Geschädigten weitere Handlungen vornimmt. Werden diese Taten zu spät oder gar nicht bemerkt, können die negativen Konsequenzen für die attackierte Person oder Körperschaft nicht nur zeitlich unmittelbar folgen, sondern sich über Jahre hinziehen.

Wird ein Cyberangriff bemerkt, sollte schnell und umfassend gehandelt werden, um weiteren Schaden zu vermeiden. Bild: Fotolia

So kann ein geprellter Onlinehändler seine Geldforderungen gerichtlich geltend machen. Der attackierte Eigner würde aufgrund der nicht gezahlten Rechnungen an den geprellten Onlinehändler einen Eintrag im Betreibungsregister erhalten, was zu negativen Bonitätsauskünften führt. Aber auch die Kosten eines Rechtsbeistandes bei eventuellen gerichtlichen Auseinandersetzungen sind nicht zu vernachlässigen.

Was ist bei einer Attacke zu unternehmen?

Bemerkt eine Person oder Körperschaft einen solchen Cyberangriff, sollte schnell und umfassend gehandelt werden, um weiteren Schaden abzuwenden. Hierzu ist es zwingend erforderlich, sowohl die Polizei als auch die Anbieter des sozialen Netzes oder internetgestützten Angebots zu kontaktieren, wobei folgende Aspekte berücksichtigt werden sollten.

(1) Zunächst sollte die attackierte Person/Körperschaft alle Konten bei allen (also auch den anderen) Onlineangeboten mit neuen Zugangs- und digitalen Kontaktdaten (E-Mails) versehen. (2) Anschliessend sollten sowohl online im eigenen angegriffenen Profil, Blog, Wiki etc. als auch real die nahestehenden Personen/Körperschaften sachlich über die Attacke oder den Identitätsdiebstahl und den damit betriebenen Missbrauch informiert werden. Hierdurch können eventuelle Missverständnisse oder Fehlhandlungen (beispielsweise die Annahme von Paketlieferungen durch den Nachbarn, die aus vorgetäuschten Warenbestellungen stammen) gar nicht erst aufkommen. (3) Der Betreiber des betroffenen Onlinekontos ist ebenfalls zu unterrichten, damit er die Handlungen, die im Namen der geschädigten Person/Körperschaft durchgeführten wurden, zwecks Beweissicherung archivieren kann. Auch kann er gefälschte Postings sperren und aus den Suchindizes entfernen.

Besonders bei schwerwiegenden Fällen ist zu prüfen, ob vom Cyberkriminellen strafrechtlich relevante Taten vorgenommen wurden. Ist dies der Fall, ist umgehend Anzeige bei der Polizei zu erstatten. Sowohl für die eigenen als auch für eventuelle strafrechtliche Ermittlungen ist es wichtig, zu überlegen und mitzuteilen, wer der Cyberkriminelle sein könnte. Zumeist sind dies Personen/Körperschaften, die in einem direkten Zusammenhang zur angegriffenen Person/Körperschaft stehen. Auch wenn keine strafrechtlich relevanten Handlungen des Cyberkriminellen vorliegen, ist es sinnvoll, die Polizei vom Cyberangriff zu unterrichten. Denn diese könnten bereits ähnliche Handlungen vorgenommen haben oder noch planen. Ein solches Muster könnte die Identifizierung von Cyberkriminellen durch die Ermittlungsbehörden vereinfachen. Die Anzeige dient aber auch zum eigenen präventiven Schutz bei tatsächlich ausgeübten Straftaten.

Was sind präventive Schutzmassnahmen?

Neben dem Berücksichtigen der hinlänglich bekannten Sicherheitsmechanismen zur Herkunft und Übermittlung von Daten sowie dem Handling von sensiblen Informationen (insbesondere von Zugangsdaten) sollte besonders in sozialen Netzen überprüft werden, welche Daten welchem Personenkreis oder gar der Öffentlichkeit zur Verfügung gestellt werden. Daten, die besonders zur Rekonstruktion von Passwortfragen, Kontaktadressen oder Zahlungsdaten hilfreich sein können, sollten nicht öffentlich gemacht werden. Bestenfalls sollten solche Daten gar nicht in sozialen Netzen und internetgestützten Anwendungen erscheinen, wenn dies nicht zwingend erforderlich ist. Ebenfalls sind die Privatsphäre-Einstellungen von Konten in sozialen Netzen regelmässig zu überprüfen und die Anzeige der Profilseiten für die verschiedenen Zielgruppen (Öffentlichkeit vs. geschlossene Nutzergruppen) zu kontrollieren.

Unternehmen sollten darüber hinaus ihre Mitarbeiter mittels geeigneter Schulungen und Weiterbildungen für die Gefahren durch Cyberkriminalität sensibilisieren und mit den notwendigen Kompetenzen versehen, damit sie entsprechende Massnahmen zu deren Abwehr entwickeln, umsetzen, evaluieren und weitergeben können. Gleiches gilt selbstverständlich auch für Privatpersonen, besonders dann, wenn diese noch wenig Erfahrung im Umgang mit sozialen Medien haben.