Anpacken statt zuschauen

Verantwortungsvoller individueller Umgang mit digitalen Daten in Forschung und Lehre

| WOLFGANG HOMMEL | **IT-Sicherheitsvorfälle gehen oft mit Stillstand im IT-Betrieb und monatelangen Wiederaufbaumaßnahmen einher. Zum Datengau gesellen sich gern ein rechtliches Nachspiel und ein Reputationsschaden. Wie können Wissenschaftlerinnen und Wissenschaftler aktiv zur Prävention beitragen?**

Der Mensch in seinem zunehmend digitalisierten Lebensraum gilt als vielbeschäftigtes Gewohnheitstier. Er gewöhnt sich daran, wöchentlich aus den Medien über IT-Sicherheitsvorfälle bei kleinen und großen Organisationen zu erfahren. Von hochprofessionellen, neuartigen Angriffen ist oft die Rede. Wer sensible Daten und IT-Systeme nicht hinreichend geschützt hat, gibt oft zu Protokoll, chancenloses Opfer skrupelloser Angreifer geworden zu sein. Alternativ wird der Vorfall als Rettungsversuch für die eigene Reputation heruntergespielt. Details zu laufenden Ermittlungen dürfe man nicht nennen; die schnelllebige Gesellschaft vergisst hoffentlich auch schnell. Unser Gewohnheitstier wird überspitzt auf ein mentales Achselzucken konditioniert: „Da kann man wohl eh nichts machen“. Der Denkanstoß zum Transfer auf die eigene IT-Umgebung fruchtet selten – vermeintlich ist das sowieso nur ein Thema für spezialisierte Nerds. Wieso sollte sich jemand ausgerechnet für mich und meine Daten interessieren?

Doch wer forscht und lehrt, trägt Verantwortung – auch für eigene und anvertraute Daten. Niemandem kann und darf es egal sein, wenn persönliche E-Mails, Notenlisten, erstellte Gutachten, von Projektpartnern vertraulich zur Verfügung gestellte Unterlagen, teaminterne Kommunikation und noch unveröffentlichte Forschungsergebnisse ins Internet gelangen oder von Dritten ausgewertet werden. IT-Sicherheit ist aber keine Dienstleistung, die von einigen wenigen für alle anderen erbracht werden kann. Jede und jeder muss einen Beitrag leisten, nicht nur die Profis im Rechenzentrum. Ähnlich wie bei der Teilnahme am Straßenverkehr gehen Fahrlässigkeiten nur so lange gut, bis es teuer, schmerzvoll oder – hier durch katastrophale Außenwirkung – gar existenzgefährdend wird.

> »Fahrlässigkeiten gehen nur so lange gut, bis es teuer, schmerzvoll oder gar existenzgefährdend wird.«

Auf dem Boden der Tatsachen

Lassen wir uns Gewohnheitstiere nicht von Hollywood-Produktionen und so mancher Presseerklärung blenden: Die Angreifer kochen auch nur mit Wasser. In vielen adademischen Einrichtungen wird es ihnen aber leicht gemacht: Hochschulangehörige werden bislang meist nicht systematisch flächendeckend sensibilisiert, IT-Personal ist knapp und überlastet. In Kombination mit essenziellen akademischen Freiheiten und dezentralen Verantwortlichkeiten werden viele IT-Systeme ohne auf IT-Sicherheit ausgerichtete Qualitätssicherung betrieben. Kein Wunder also, dass nicht nur großen Internet-Diensten, Krankenhäusern und Gemeinden mediale Aufmerksamkeit gewidmet wird, sondern auch Hochschulen, wenn einschlägige Vorfälle publik werden. Doch wie kann man persönlich dazu beitragen, erfolgreichen Angriffen vorzubeugen und Auswirkungen zu minimieren? Was ist zu tun, wenn das Kind schon in den Brunnen gefallen ist?

Grundlegend ist zunächst ein Verständnis dafür, welche Ziele die Angreifer verfolgen. Im Fokus stehen derzeit oft zwei Angreiferkategorien: Auf der einen Seite sind es organisierte Kriminelle, die an einer direkten Monetarisierung interessiert sind. Daten werden erst vom Angreifer kopiert und dann oft auf den Systemen der Angegriffenen durch Verschlüsselung unbrauchbar gemacht, um den Leidensdruck zu erhöhen. Gegen eine Lösegeldzahlung als Kern des kriminellen Geschäftsmodells wird angeboten, großzügig auf die Veröffentlichung der erbeuteten Daten zu verzichten und den lokalen Zugriff darauf wieder zu ermöglichen. Auf der anderen Seite geht es um Spionage, also die inhaltliche Verwertung der erbeuteten Daten: Geistiges Eigentum, Kontakte und Meinungsbilder, vielleicht sogar so manche Peinlichkeit, die Einzelne zu passender Zeit erpressbar werden lässt.

AUTOR

Foto: Angelika Wagener Fotografie

Wolfgang Hommel hat die Professur für IT-Sicherheit von Software und Daten an der Universität der Bundeswehr München inne und ist leitender Direktor des Forschungsinstituts Cyber Defence (FI CODE): www.unibw.de/code.

Gelegenheit macht in beiden Fällen Datendiebe: Digital eingebrochen wird vor allem dort, wo es am einfachsten gelingt; wesentlich seltener zielt der Angriff auf nur eine ausgewählte Einzelperson und genau deren Daten.

Angriffswege und Prävention

Viele erfolgreiche Angriffe kombinieren den Faktor Mensch mit Sicherheitslücken in der Technik: Zunächst werden Zugangsdaten, beispielsweise Benutzername und Passwort, einer Person in der Zielorganisation akquiriert. Im einfachsten Fall gelingt dies mit einer hinreichend guten Phishing-E-Mail: Die Empfänger werden unter einem Vorwand aufgefordert, eine Website zu nutzen, die beispielsweise der des Rechenzentrums oder der Bibliothek gleicht und zur gewohnten Eingabe der Zugangsdaten auffordert. In Wirklichkeit wird die Website von den Angreifern betrieben und dient nur dazu, Zugangsdaten abzugreifen. Perfider sind länger angebahnte Kontakte über E-Mail oder Social-Media-Plattformen, bei denen Angreifer fingierte Profile verwenden. Über eine längere Korrespondenz wird zunächst ein Vertrauensverhältnis aufgebaut. Getarnt zum Beispiel als Bewerbung, Vorschlag für ein gemeinsames Projekt oder eine relevante Publikation wird schließlich Schadsoftware zugeschickt, mit der das Gerät des Opfers kompromittiert wird. Haben die Angreifer Zugangsdaten oder ein erstes Gerät gekapert, können sie sich im Hochschulnetz nach technisch unzureichend geschützten Systemen und interessanten Daten umsehen. Wie aus dem Homeoffice oder Büro kann dabei auch auf Systeme zugegriffen werden, die nicht direkt aus dem Internet erreichbar sind.

Das Hüten der eigenen Zugangsdaten und Geräte ist somit essenziell. Software der Kategorie Passwortmanager kann davor schützen, Zugangsdaten unbedacht auf imitierten Websites einzugeben. Damit ist etwas Einarbeitungszeit verbunden, die sich aber auch für das private Umfeld rentiert. Bei jeder Art von E-Mail-Anhängen ist eine grundsätzliche Skepsis angebracht, mindestens wenn sie unerwartet zugehen, auch wenn die meisten harmlos sind. Als dubios sollten auch verschlüsselte E-Mail-Anhänge betrachtet werden, zu denen das Passwort gleich mitgeliefert wird, oder Links auf Internet-Adressen, unter denen der Anhang heruntergeladen werden kann: Im Falle eines Angriffs sollen damit die Schadsoftware-Schutzmaßnahmen der E-Mail-Server umgangen werden.

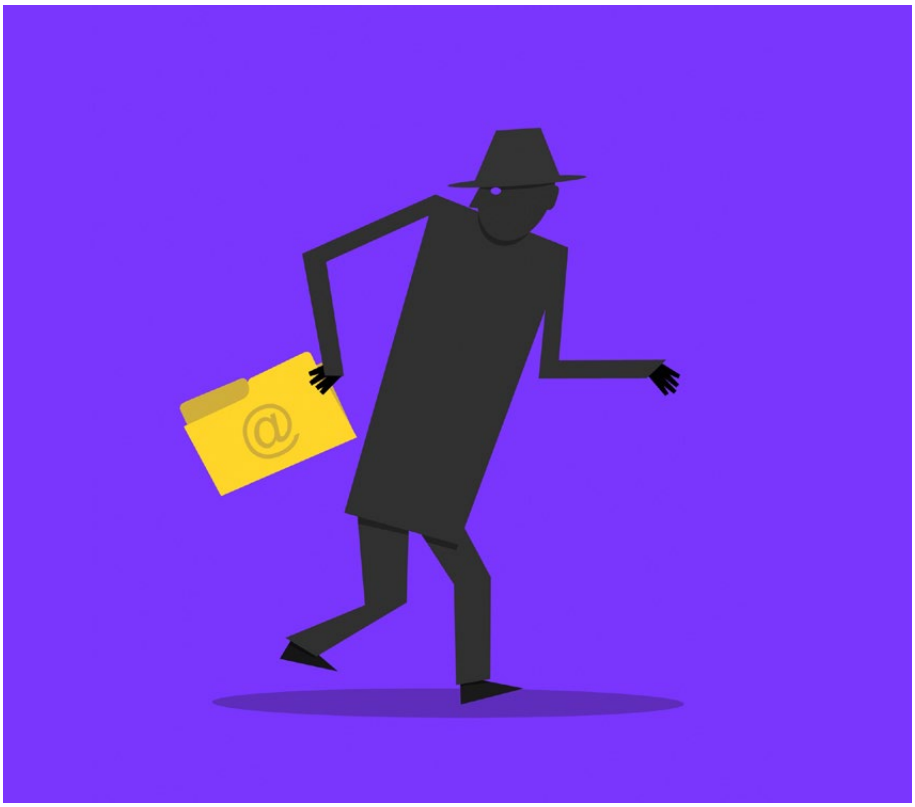

Foto: mauritius images / Ikon Images

Für die weitere Präventionsplanung hat es sich bewährt, davon auszugehen, dass Angreifer bereits Zugangsdaten erbeutet haben – die eigenen, eines Teammitglieds oder einer Person im Nachbargebäude. Wie leicht haben es die Angreifer jetzt? Sind die Zugriffsberechtigungen auf zentrale Dateiablagen so eingerichtet, dass jeder an alle Daten kommt, oder sind sie nur an diejenigen vergeben worden, die sie z.B. im eigenen aktuellen Forschungsprojekt wirklich benötigen? Sind noch Geräte oder Dienste online, die von bereits ausgeschiedenem Personal für ein längst abgeschlossenes Projekt betrieben wurden? Handhaben Sie Ihre eigene IT-Infrastruktur und Daten wie Ihren Schreibtisch: Alles, was länger nicht benötigt wird, kann offline archiviert oder gar entsorgt werden und entzieht sich somit auch dem einfachen Zugriff durch Angreifer. Machen Sie sich Datenhygiene zur Gewohnheit: Das erste Mal dauert länger, schnell stellt sich Routine ein.

Professioneller Umgang

Leider ist kein noch so bemühter Schutz perfekt. IT-Sicherheitsvorfälle können eintreten und müssen schnellstmöglich strukturiert behandelt werden, bevor sie sich ausweiten. Jede Hochschule sollte sich den prinzipiellen Ablauf vorab überlegen, damit im Ernstfall kein Chaos ausbricht. Wie werden Vorfälle gemeldet? Wer übernimmt die technische Analyse? Wer prüft wie die datenschutzrechtliche Relevanz? Wann werden Leitungsgremien einbezogen und weitere Betroffene informiert? In welchen Fällen werden wann welche Behörden kontaktiert? Wie wird mit Kontaktaufnahme von außen umgegangen, von der Lösegeldforderung bis zur Presseanfrage? Das festgelegte Vorgehen muss allen Hochschulangehörigen auch bekannt sein. Wenn dies bei Ihnen nicht zutrifft, fragen Sie freundlich fordernd nach. Die Verantwortlichen sollten Ihnen dafür dankbar sein: Zur öffentlichen Blamage trägt ein unprofessioneller Umgang mit Sicherheitsvorfällen ganz wesentlich bei.

Wir Gewohnheitstiere sorgen also daheim für Ordnung und gehen sensibilisiert auf Reisen. In einigen Ländern können bereits bei der Einreise Kopien von Daten auf mitgeführten Geräten angefertigt und die Preisgabe von Passwörtern erzwungen werden. Nicht jedes Hotel ist ein sicherer Aufbewahrungsort, Internet-Verbindungen werden überwacht, Verschlüsselung verboten. Kleine Gastgeschenke wie USB-Sticks können schön anzusehen sein, aber auch Schadsoftware enthalten. Wer viel reist, gewöhnt sich leichtes Gepäck an – auch bei den Daten.