Im Wettrüsten mithalten

Strategien zur Abwehr von Cyberangriffen | Jeder und jede kann Ziel einer Cyberattacke werden. Da die Angreifer ihre Methoden ständig weiterentwickeln, sehen sich die potenziellen Opfer permanent mit neuen Bedrohungen konfrontiert. Doch auch die Möglichkeiten zur Abwehr werden immer besser.

ENDRE BANGERTER, BRUCE NIKKEL

Um gegen zukünftige Bedrohungen gewappnet zu sein, lohnt sich bisweilen ein Blick in die Vergangenheit. Das gilt auch beim Thema Cybercrime. Vor etwa 15 Jahren gehörten Bankkunden zu den ersten Opfern von Kriminellen, die versuchten, sich mit Trojaner-Programmen Zugriff auf das Internet-Banking zu verschaffen. Heute sind die Banken besser in der Lage, infizierte Kunden-Computer zu entdecken und Cyberangriffe rechtzeitig abzuwehren. Cyberkriminelle sind meistens Opportunisten. Wenn der Widerstand zu stark ist, suchen sie sich ein anderes Opfer oder ein neues Schlupfloch. So haben sie seit einigen Jahren vermehrt Firmen jeder Grösse und Branche mit Ransomware ins Visier genommen. Dabei ist häufig das gesamte IT-Netzwerk eines Unternehmens betroffen. Für die Freigabe der gehackten Daten versuchen die meistens aus dem Ausland operierenden Banden, ein Lösegeld in der Bitcoin-Währung zu erpressen. Die Fahndung nach den Tätern ist aufwendig und selten erfolgreich.

Menschen statt Maschinen hacken

Eine zunehmende Bedeutung hat Social Engineering, was sich mit «sozialer Manipulation» übersetzen lässt. Angreifer profitieren dabei von menschlichen Eigenschaften wie der Arglosigkeit. Es ist erstaunlich, wie viele Firmen ohne Not Informationen

Bild: BFH

preisgeben, die Eindringlingen Türen öffnen. Wenn etwa ein Job-Beschrieb auf der Firmenwebseite darüber Auskunft gibt, welche Software im Unternehmen im Einsatz ist, lässt sich das ausnützen – zum Beispiel indem sich ein Angreifer am Telefon als Mitarbeiter des Software-Herstellers ausgibt und ankündigt, er werde gleich ein Dokument mit wichtigen Update-Informationen schicken. Wird die Täuschung glaubhaft vorgebracht, öffnet der Empfänger möglicherweise das Dokument und gewährt einer Malware Zutritt ins Firmennetzwerk. Die Schwachstelle im System war dann nicht die Technik, sondern der Mensch. Ebenfalls zum Social Engineering gehören mit Methoden der künstlichen Intelligenz manipulierte Videos, in denen Gesichter verändert werden (Deepfakes). Damit kann man eine beliebige Person Dinge sagen lassen, welche diese Person in der Realität nie von sich gegeben hätte.

Vertrauen allein genügt nicht

Die Vernetzung in der digitalen Welt und die damit verbundenen gegenseitigen Abhängigkeiten eröffnen Hackern immer neue Möglichkeiten. Schlagzeilen machte der Fall des auf Netzwerkmanagement-Software spezialisierten US-Unternehmens Solarwinds. Wegen eines schwachen Passworts auf einem Updateserver konnten im Jahr 2019 Angreifer Schadprogramme in ein Softwareprodukt der Firma einschleusen und monatelang unentdeckt Kunden von Solarwinds ausforschen – eine klassische «supply chain attack». Eine einzige Sicherheitslücke am Ursprung der Lieferkette genügte in diesem Fall, um alle davon abhängigen Systeme zu infiltrieren. Die Erkenntnis aus diesem Vorfall lautet: Vertrauen ist gut, im Cyberspace aber nicht gut genug. Das gilt auch dann, wenn man Datenverarbeitung outsourct oder auf cloudbasierte Lösungen setzt. Dabei sollte gründlich geprüft werden, ob der externe Partner anerkannte Sicherheitsstandards erfüllt. Zudem sollten die gesetzlichen Bestimmungen des Landes beachtet werden, in denen der Partner seinen Geschäftssitz hat oder die anvertrauten Daten verarbeitet. Amerikanische IT-Dienstleister etwa sind von Gesetzes wegen verpflichtet, den US-Behörden Zugriff auf gespeicherte Daten zu gewähren («Cloud Act»), sogar wenn diese aus dem Ausland stammen.

Resignation ist keine Option

Unternehmen und Institutionen haben in den vergangenen Jahren gelernt, mit der Cyberkriminalität umzugehen. Das Bewusstsein, dass man jederzeit Zielscheibe eines Angriffs werden kann, ist gestiegen. Bei der Planung von Vorsorgemassnahmen stellt sich dennoch die Frage nach dem richtigen Verhältnis zwischen Aufwand und Nutzen. Hochstehende Technologien bieten einen guten Schutz, kosten aber viel Geld. Und absolute Sicherheit können auch sie nicht bieten. Deswegen den Kopf in den Sand zu stecken, ist dennoch die schlechteste Option. Angreifer und Verteidiger liefern sich ein permanentes Wettrüsten mit wechselnden Vorteilen für die eine oder die andere Seite. Damit wird man weiterhin leben müssen. Der IKT-Minimalstandard des Bundes kann dabei helfen, den Handlungsbedarf im eigenen KMU zu ermitteln und Abwehrmassnahmen zu planen.

Herausforderung Datenanalyse

Wer immer noch glaubt, mit einer Firewall und einem Antivirenprogramm Angreifern den Zugang zum Firmennetzwerk zu verunmöglichen, muss jedenfalls umdenken. Wirksame Abwehrmassnahmen erfordern eine permanente Überwachung aller Systeme und Netzwerke. Die grosse Herausforderung besteht darin, die grossen Datenmengen rasch zu verarbeiten. Dies ist Voraussetzung, um Gegenmassnahmen einleiten zu können, bevor die Malware Schaden anrichtet. Ein innovativer Ansatz besteht darin, die Daten mit Methoden des «Machine Learning» zu analysieren. Die meisten Schadprogramme sind nicht vollständig neu entwickelt, sondern verwenden einzelne Komponenten aus bereits existierender Malware. Diese müssen allerdings erst aufgespürt werden, was mit einer manuellen Analyse sehr aufwendig und teuer ist. Mit einem vom BFH-Spin-off «Threatray» entwickelten Analysetool ist es nun möglich, automatisch und in kürzester Zeit Korrelationen von einer Vielzahl von Samples zu prüfen. Dazu muss es laufend mit allen verfügbaren Informationen über bereits bekannte Schadprogramme gefüttert werden.

Vom Wissen der anderen profitieren

Ein immer wichtigerer Faktor für die Abwehr von Cyberangriffen ist der Austausch von Wissen und Informationen auf nationaler und internationaler Ebene. Fast jede Branche bildet heute «Threat intelligence Communities» – Teams von Spezialisten der Mitglieder, die sich den gemeinsamen Herausforderungen stellen. Im Fall der Elektrizitätsversorger beispielsweise ist dies das EE-ISAC («European Energy – Information Sharing & Analysis Center»). Es stellt Basisinformationen und Handlungsempfehlungen auch Nichtmitgliedern zur Verfügung. Ausserdem sollten sich Unternehmen und Organisationen das Know-how der Schweizer Bildungsinstitutionen zunutze machen. Die technischen Hochschulen sowie verschiedene Universitäten und Fachhochschulen sind in den Bereichen Cyber-Security und digitale Forensik tätig. Laufend kommen neue Bildungsangebote dazu, 2020 etwa der Studiengang MAS Digital Forensics & Cyber Investigation der Berner Fachhochschule. Das dabei akkumulierte Know-how steht privaten Partnern für die Entwicklung von Praxisanwendungen zur Verfügung.

Autoren

Prof. Dr. **Endre Bangerter** ist Co-Leiter des Institute for Cybersecurity and Engineering (ICE).
→ BFH, 2501 Biel
→ endre.bangerter@bfh.ch

Prof. Dr. **Bruce Nikkel** ist Co-Leiter des Institute for Cybersecurity and Engineering (ICE).
→ bruce.nikkel@bfh.ch