Cyber-Kriminalität

Angriff von innen

Unterschätzte Gefahr: Bei Datendiebstahl und Attacken auf die betriebliche IT sind oft Mitarbeiter die Täter.

Passwörter, Zugriffsberechtigungen, Verschlüsselungen: Bei den meisten Unternehmen ist angekommen, dass der Schutz der betrieblichen IT-Infrastruktur und der betrieblichen Daten jede Mühe wert ist. Dies ist angesichts der möglichen Folgen auch mehr als angebracht: So berichtet der Branchenverband Bitkom, dass allein der Industrie durch Sabotage, Datendiebstahl und Spionage in den vergangenen zwei Jahren ein Gesamtschaden von 43,4 Mrd. Euro entstanden ist.
Allerdings gehen die meisten Betriebe irrtümlicherweise davon aus, dass nur von außen Gefahr droht. Aber die meisten erfolgreichen Angreifer kommen aus dem eigenen Unternehmen und knacken die virtuelle Festung mit ihrem Insider-Wissen von innen. Das bestätigen auch unterschiedliche Untersuchungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Bundeskriminalamtes (BKA) und von IT-Forensikern: Demnach kommen – je nach Quelle und Studie – zwischen 60 und 90 Prozent der gelungenen Angriffe auf Unternehmen nicht von außen, sondern

Dieses Dokument wurde automatisch generiert aus den Onlineinhalten der Industrie- und Handelskammer Nürnberg für Mittelfranken http://www.ihk-nuernberg.de

werden durch eigene Mitarbeiter ausgeführt. „Die Hauptgefahr, Opfer krimineller Handlungen zu werden, liegt also in einer komplett unterschätzten Quelle“, warnt Axel Bernhardt, Kriminalitätsexperte und Inhaber eines IT-Forensik-Unternehmens.

Als Beispiel ein Fall, der sich in ähnlicher Weise tatsächlich so zugetragen hat: Frank M. führt ein Unternehmen, das Kfz-Teile herstellt, und erfährt von einem Kunden, dass seine Produkte auch auf Ebay angeboten werden – und zwar unter dem Ladenpreis. Frank M. ist das nicht bekannt, er beginnt, im eigenen Unternehmen nachzuforschen. Einen Diebstahl kann er durch eine Bestandskontrolle schnell ausschließen. Bei einem Testkauf stellt sich heraus, dass der Verkäufer ein Angehöriger des Vertriebsmitarbeiters Michael L. ist. Die Auswertung seines dienstlichen Notebooks ergibt, dass er mit seinem Verwandten kommuniziert und ohne Berechtigung auf das Produktionsplanungs- und Warenwirtschaftssystem zugegriffen hat. Zudem sammelte er Kundenlisten sowie Produktionsunterlagen und CNC-Programme, zu denen er keinen Zugang haben sollte. Die Auswertung des Zeiterfassungs- und Zugangssystems zeigte, dass Michael L. und ein Administrator mehrfach zeitgleich und außerhalb der normalen Arbeitszeiten in der Firma waren. Es wurde klar, dass der Administrator die Zugänge zu den sensiblen Daten für Michael L. eingerichtet und die Berechtigung für manuelle Korrekturen und Änderungen freigeschaltet hatte. Letztlich stellte der Firmeninhaber fest: Seine Waren wurden durch Manipulation des Produktionsplanungssystems überproduziert und durch unberechtigten Eingriff in das Warenwirtschaftssystem ausgetragen. Anschließend wurden sie vom Angestellten Michael L. über dessen Mittelsmann auf Ebay verkauft – ohne das Wissen des Unternehmers und ohne Einnahmen für ihn. Damit nicht genug: Auf dem Notebook des Vertrieblers fanden sich E-Mails, die erkennen ließen, dass Michael L. einen noch größeren Plan verfolgte – er wollte mit den illegal erlangten Produktionsunterlagen und CNC-Programmen eine eigene Produktion starten.

Die Vorteile der Digitalisierung entlang der gesamten Wertschöpfungskette liegen auf der Hand: mehr Effizienz, Transparenz, beschleunigte Prozesse, stärkere Automatisierung etc. Sie birgt aber auch zwei Gefahren: Erstens werden Unternehmen immer abhängiger von einem funktionierenden IT-System. Zweitens befinden sich immer mehr und teilweise hoch sensible Daten im Netz. Das machen sich Kriminelle zunutze, die sowohl von außen als auch von innen angreifen.

Die Formen der Kriminalität von „Innentätern“ sind vielfältig: Korruption, Untreue und Insiderhandel gehören dazu. Weitere Beispiele für gängige Straftaten sind der Verkauf von Betriebsgeheimnissen, die Weitergabe von Kunden- oder Auftragsdaten, Produktpiraterie sowie die Manipulation von Waren- und Finanzströmen. Im Wesentlichen verfolgen die Angreifer folgende Ziele: Spionage, Erpressung und Veräußerung von Daten.

Spielarten der Cyber-Kriminalität

Die Szenarien, wie diese kriminellen Aktivitäten aus dem eigenen Haus heraus vonstatten gehen, sind vielfältig: Administratoren könnten ihre Macht missbrauchen und sich verbotene Zugänge verschaffen. Andere Mitarbeiter sperren die Zugänge zu den betrieblichen Datennetzen und erpressen damit ihre Arbeitgeber, wobei sowohl die IT-Systeme als auch die Daten das Ziel der Angriffe sein können. Denn die Daten sind die Grundlage für fast alle betrieblichen Prozesse. Ihr Verlust oder ihre Nichtverfügbarkeit ist daher für Unternehmen ein fundamentales Problem, das sie erpressbar macht. Daten, die gestohlen werden und in falsche Händen geraten, können beispielsweise die Wettbewerbsfähigkeit des betroffenen Unternehmens massiv schwächen. Hinzu kommt, dass gerade personenbezogene Daten einem strengen gesetzlichen Schutz unterliegen. Wenn sie von Unbefugten abgegriffen werden, drohen den betroffenen Unternehmen neben behördlichen Ermittlungen auch Strafzahlungen, Schadenersatzansprüche und nicht zuletzt ein massiver Imageschaden.

Technische Maßnahmen wie ein effizienter Passwortschutz auf allen Geräten sowie Systeme zur Erkennung und Abwehr von Angriffen (Intrusion Detection- und Intrusion Prevention-Systeme) sind wichtig und unbedingt

Dieses Dokument wurde automatisch generiert aus den Onlineinhalten der Industrie- und Handelskammer Nürnberg für Mittelfranken http://www.ihk-nuernberg.de

empfehlenswert, schützen aber nur eingeschränkt vor „Innentätern“. Diese verfügen nämlich häufig über die notwendigen Zugriffsrechte oder das Wissen, wie Schwachstellen im Unternehmen umgangen werden können. Besonders aufmerksam sollten Firmen sein, wenn externe Fachkräfte oder Dienstleister in ihrem Betrieb tätig sind. Deren Hemmschwelle ist noch einmal deutlich geringer. Ebenfalls ein großes Problem für Unternehmen sind aktive – aber auch versehentliche – Verletzungen von Geheimhaltungsverpflichtungen und Vertraulichkeitsverletzungen gegenüber Dritten.
Die IT-Sicherheit liegt im Eigeninteresse der Geschäftsleitung und sollte daher von dieser auch aktiv gemanagt werden. Denn IT-Sicherheitsverletzungen können großen wirtschaftlichen Schaden anrichten und die Existenz eines Unternehmens gefährden. In allen Fällen drohen neben Imageschäden und Auftragsverlusten oft auch empfindliche Vertragsstrafen. Außerdem sieht sich die Geschäftsleitung dem Vorwurf eines Organisationsverschuldens ausgesetzt, wenn sich herausstellt, dass Betriebsprozesse und Sicherungsmaßnahmen nicht ausreichend waren. Wichtig ist deshalb, klare Regeln für den Umgang mit schützenswerten Informationen aufzustellen und eine zuverlässige Daten-Sicherheitsstruktur einzurichten. Unverzichtbar sind auch (Online-)Schulungen der Mitarbeiter in Sicherheitsthemen, wie sie von manchen Cyber-Police-Anbietern kostenfrei angeboten werden.

Cyber-Policen

Für die neuen Risiken gibt es auch neue Formen der Absicherung: So können sich Unternehmen mit Cyber-Policen vor den finanziellen Folgen einer sogenannten Netzwerksicherheitsverletzung schützen, sogar bis hin zu kompletten Betriebsstillständen. Neben der rein finanziellen Entschädigung bieten die Policen je nach Anbieter einige interessante Zusatzdienste, wie z. B. die Unterstützung durch IT-Forensiker sowie Rechts- und PR-Beratung. Vertragsstrafen nach Vertraulichkeitsverletzungen oder verzögerter Leistungserbringung sind mittlerweile ebenfalls versicherbar. Die Nachfrage nach diesem speziellen Schutz hat aus guten Gründen stark zugenommen. Allerdings sind die Leistungsunterschiede der am Markt angebotenen Konzepte sehr groß. Allen gemein sind die engen Grenzen, was die Deckung der Vermögensschäden durch Betrug angeht. Möchten sich Unternehmen auch dagegen absichern, ist dies mit einer geeigneten Kombination aus Cyber- und Vertrauensschadenversicherung möglich.

Autor: Martin Trescher ist Geschäftsführer der Versicherungsmakler Adlatus GmbH in Weißenburg (cyberschutz@adlatus.info).
WiM - Wirtschaft in Mittelfranken, Ausgabe 03/2019, Seite 38

Dieses Dokument wurde automatisch generiert aus den Onlineinhalten der Industrie- und Handelskammer Nürnberg für Mittelfranken http://www.ihk-nuernberg.de