«Unsere Daten sind sicher»

CYBER SECURITY Der Schweizer Industrie entstanden in den letzten Jahren Schäden in Milliardenhöhe durch ausspionierte, sabotierte oder gestohlene Daten. elleta und Compass Security berichten, wie sie in einem gemeinsamen Projekt ein Unternehmen zu einer Datenfestung machten.

INTERVIEW RUEDI STRICKER

Herr Hasler, was für Unternehmen sind am meisten exponiert?
Grundsätzlich kann es jede Organisation treffen. Im Fall von Spionage sind mittlere Industrieunternehmen besonders gefährdet. Sie verfügen einerseits über technisches Know-how, das für Mitbewerber interessant ist, und haben andererseits wenig in den Schutz dieser Werte investiert. Zudem fällt im Unterschied zu einem Angriff mit destruktiven Motiven ein solcher Angriff nicht einmal auf. Das Opfer stellt nur irgendwann fest, dass ein Mitbewerber seine Produkte auffallend schnell und geschickt kopiert, bleibt aber in Bezug auf die Ursache ahnungslos.

Wer sind die Täter?
Je nach Motiv treffen wir hier auf verschiedenste Gruppen. Das Spektrum reicht vom Auftragshacker, der diskret Informationen über technische Verfahren oder Kundendaten absaugt, bis zum frustrierten Mitarbeiter, der sich an seinem ehemaligen Arbeitgeber rächt. Da hat doch tatsächlich letztes Jahr eine KMU vergessen, Login und Passwörter eines Ehemaligen zu löschen, obwohl dieser sogar konkret mit Vergeltung gedroht hatte. Aber in zahlreichen Fällen gibt es ja nicht einmal einen böswilligen Täter. Bei unserer Arbeit stossen wir auch auf scheinbar Banales wie das Fehlen von geeigneten Feuerlöschern in Serverräumen oder auf Backups, die im gleichen Raum gelagert werden wie die Originaldaten.

Welches sind die häufigsten Angriffsziele?
Ein Angriff erfolgt direkt via Netz auf die Infrastruktur oder via Social Engineering: Bei Letzterem geht man davon aus, dass es in jeder Organisation menschliche «Schwachstellen» gibt, wo Nichtwissen oder Mangel an gesundem Misstrauen das Vorgehen erleichtern. In den meisten Fällen kommt es dabei nicht zu Delikten wie Bestechung oder Erpressung. Ein geschickter Täter erreicht sein Ziel schon durch kleine Aufmerksamkeiten oder ein paar harmlos klingende Fragen in lockerer Atmosphäre.

Was unternimmt der Staat dagegen?
Das Schweizer Bundesamt für wirtschaftliche Landesversorgung (BWL) lanciert derzeit einen Minimalstandard zur Verbesserung der IKT-Resilienz mit erhöhtem Fokus auf Vorfallsbehandlung (Incident Response). Die entsprechende Publikation richtet sich zwar insbesondere an die Betreiber von kritischen Infrastrukturen, ist aber grundsätzlich für jedes Unternehmen oder jede Organisation anwendbar. Im Fürstentum Liechtenstein hat die FMA Finanzmarktaufsicht kürzlich in einem Schreiben an die Marktteilnehmer ihre Erwartungen zum Umgang mit Cyber-Risiken konkret formuliert.

Und was empfehlen Sie?
Staatliche Empfehlungen, so sinnvoll sie sind, können nicht auf einzelne Situationen eingehen. Zudem machen wir die Erfahrung, dass eine Unternehmung mit Vorteil eine gesamthafte Betrachtung vornimmt. Es gibt neben der reinen Sicherheit der Daten auch noch den Datenschutz, also die Rechte von Personen an ihren Daten, sowie weitere Themen wie Enterprise Risk Management. Zudem muss das Ganze ja auch finanzierbar sein. Unser Ziel ist jeweils, basierend auf den Bedürfnissen und Möglichkeiten des Kunden, ein angemessenes Schutzniveau herzustellen.

Erzählen Sie bitte von Ihrem letzten Projekt!
Unser Kunde, ein grösseres Unternehmen, hat uns mit dem Aufbau eines Information Security Management Systems beauftragt. Damit verbunden war die Abgrenzung zum Thema Datenschutz, die Vorbereitung auf eine Zertifizierung nach ISO 27001 und umfangreiche Sicherheitsprüfungen. Vor dem Projektstart haben wir gemeinsam und mit Unterstützung seitens Compass Security festgelegt, welches die kritischen Systeme und Prozesse sind und welcher Sicherheitslevel sinnvoll und wirtschaftlich zu rechtfertigen ist.

Warum sind zwei Firmen für so ein Projekt nötig?
elleta ist als IT-Beratungsunternehmen an sich schon recht spezialisiert. Wir haben uns seit der Gründung auf die Kombination von technischem, organisatorischem und juristischem Know-how konzentriert. Das kam uns in den letzten Jahren im Zusammenhang mit der Verschärfung der Datenschutzgesetzgebung sehr entgegen. Aber im vorliegenden Fall reicht das nicht aus. Durch die Mitwirkung von Compass Security verfügen wir über spezialisiertes Know-how dort, wo mit krimineller Energie und hohem Einsatz versucht wird, in Systeme einzudringen. Was wir tun, kann weder eine Anwaltskanzlei noch ein Datenschutzspezialist noch ein Informatiker oder ein Forensiker allein.

Ihre Freunde haben als «friendly hackers» gezielt Angriffe vorgenommen.
Ja. Compass Security prüft mit den Techniken eines Angreifers die Verletzlichkeit von Systemen und die Effektivität des Abwehrdispositivs. So stossen sie beispielsweise auf verschlüsselten Internetverkehr, der nicht nach Schadcode durchsucht wird. Oder es finden sich fehlkonfigurierte Systeme, mit welchen ein Cyberkrimineller erhöhte Privilegien und somit Zugriff auf die Kronjuwelen der Unternehmung erhält. Manchmal sind interne Dienste aus Versehen im Internet exponiert. Bei solchen Fällen sind nicht nur Daten betroffen, sondern Anlagen und Geräte. Zum Beispiel industrielle Steuerungen, Medizinaltechnik, Hochregalsysteme, Schliessanlagen, Zutrittskontrollsysteme, Kühlanlagen, Videoüberwachung oder die Telefonie.

Was hat Ihr Kunde am Schluss des Projekts in der Hand?
Das Unternehmen hat anhand einer GAP-Analyse entschieden, wo gezielt in die Sicherheit zu investieren ist. Es verfügt jetzt über qualifizierte Informationen über den aktuellen Sicherheitslevel und hat die organisatorischen Hausaufgaben gemacht. Die Mitarbeitenden sind geschult und sensibilisiert. Und in den meisten Fällen können wir feststellen, dass durch unseren unternehmensübergreifenden Ansatz Synergieeffekte realisiert und damit Kosten gespart wurden.

ÜBER ELLETA

elleta ist ein spezialisiertes Beratungsunternehmen mit ausgeprägter Erfahrung im Security-, Compliance- und Risikobereich sowie mit starken Wurzeln im Digital- und IT-Umfeld. Für die Durchführung von Cybersecurity-Projekten, IT-Audits und die Erfüllung der Anforderungen aus der europäischen Datenschutzgrundverordnung nutzt elleta das langjährige Fachwissen ihrer Experten sowohl bei Regulierungsthemen als auch im Digital-/IT-Umfeld.
Das Unternehmen erbringt seine Dienstleistungen für Kunden im schweizerisch/liechtensteinischen Markt, international ausgerichtete Firmen und für lokale Klein- und Mittelbetriebe. elleta hat ihren Firmensitz in Balzers, Liechtenstein mit einem zusätzlichen Standort in München. elleta München versteht sich als Kompetenzzentrum für die technologiegetriebene Transformation von Unternehmensstrukturen.

elleta AG
FL-9496 Balzers
support@elleta.net
+423 388 03 55
www.elleta.net

ÜBER COMPASS SECURITY

Compass Security ist ein renommiertes Schweizer Unternehmen, das sich auf Penetrationstests, Security Assessments, 24/7 Incident Response, digitale Forensik und Sicherheitstrainings spezialisiert hat. Die Forschungs- und Community-Beiträge von Compass Security finden regelmässig internationale Anerkennung. Darüber hinaus unterstützt das Unternehmen europäische Länder bei der Talentsuche und stellen Universitäten über vier Kontinente hinweg eine Laborumgebung für praktische Übungen zum Thema Cybersecurity zur Verfügung.

Nicht immer sind Cyber-Kriminelle die Ursache des Datenlecks, auch frustrierte Mitarbeiter können Unternehmen gefährden. Foto: iStock/ismagilov

ZUR PERSON

Alexander Hasler ist Consultant und Projektleiter bei der elleta AG mit den Schwerpunkten Informationssicherheit, Datenschutz und Business Prozess Engineering. Seine berufliche Erfahrung im IT- und Informationssicherheitsbereich erwarb er sich in mehreren Unternehmen im Bereich Telekommunikation, Finanzdienstleistung und Industrie. Er absolvierte Studien im Bereich Wirtschaftsinformatik und Business Administration.