Wer kann sich heute überhaupt noch ein adäquates Security Team leisten?

Durch die veränderte Bedrohungslage und aufgrund der wachsenden Erkenntnis, dass man sich heute kaum mehr gegen Attacken schützen kann, ist ein Umdenken im Bereich der Informationssicherheit notwendig. Die Thematik hat so stark in Komplexität und Themenbreite zugenommen, dass es einem Menschen oder einem kleinen Team kaum mehr möglich ist, eine Unternehmung adäquat gegen die IT- und Cyberbedrohungen zu schützen. Es braucht neue Sourcing-Modelle, bei denen auf ein grosses Team von Security-Spezialisten flexibel und bedarfsgerecht zugegriffen werden kann.

Für lange Jahre ging das Modell für viele Unternehmen auf: Um die Thematik "IT Security" in den Griff zu bekommen, stellt man einen Security Officer (CISO) ein. Dieser, zusammen mit seinem Team, kümmert sich um alle Belange der IT Security und stellt sicher, dass das Unternehmen mit seinen Prozessen von schädlichen Viren und Hackern verschont bleibt. Oft wird diese Verantwortung als Nebenaufgabe vom Netzwerkteam übernommen - Firewalls sind ja schliesslich Netzwerkkomponenten. Das macht auch Sinn.

Die Zeiten haben sich jedoch verändert. Unsere Geschäftsprozesse sind heute so stark digitalisiert und von Informationstechnologie abhängig, dass auch nur eine reduziert leistungsfähige IT nicht mehr ausreicht, um akzeptabel die unternehmerischen Leistungen erbringen zu können. Immer mehr sind Kernprozesse von Unternehmen direkt von einer funktionierenden IT abhängig. Und auch vor diesen Prozessen machen Optimierungsgedanken in Bezug auf "Cloud Computing" keinen Halt.

Für Security Teams erschwerend hinzu kommt die Komplexität. Eine wichtige Security-Regel, welche auch heute noch Gültigkeit hat, besagt, dass Komplexität der Feind der Security ist. Und genau diese Komplexität steigt aktuell überdimensional. Einerseits ist dies die technische Komplexität der informationsverarbeitenden Systeme, andererseits aber auch die gesetzliche Komplexität, welche durch die steigende Internationalisierung der Geschäftsprozesse entsteht. Immer mehr Unternehmen müssen, um weiter erfolgreich am Markt bestehen zu können, über die Landesgrenzen der Schweiz hinausschauen und im Ausland zusätzliche Absatzkanäle finden. Die gesetzlichen Auflagen und deren Implikationen auf die technische Infrastruktur steigen dabei massiv an. Hinzu kommen steigende Anforderungen der Mitarbeitenden an einen modernen Arbeitgeber: Bring your own device, work from home, mobile computing und viele weitere Ansätze werden heute praktisch vorausgesetzt.

Gleichzeitig vollzieht sich auf der „dunklen Seite“ eine Transformation der Geschäftsmodelle. Während früher der junge, schlecht ernährte und aufgrund von Tageslichtmangels schlecht gebräunte Mann mit Kapuzenjacke das typische Bedrohungsbild war, ist es heute ein technischer Spezialist, welcher sich jeden Morgen zu seinem

Arbeitgeber begibt, um in dessen Auftrag andere Firmen anzugreifen. Die Cyberkriminalität hat sich zu einem Industriezweig entwickelt. Der Grund hierfür ist, dass sich durch Hacking viel Geld verdienen lässt. Dabei kann es sich um offengelegte Geschäftsgeheimnisse handeln oder um die Erpressung von Unternehmen durch Verschlüsselung ihrer Daten. Der Umsatz von Cyberkriminalität wird weltweit auf zwischen 300 Milliarden und eine Trillion Dollar im Jahr geschätzt - mehr als mit Drogenhandel verdient wird.

In einer Welt, in der unsere Geschäftsprozesse und somit der erfolgreiche Bestand einer Unternehmung direkt von einer stabil funktionierenden IT Infrastruktur abhängen, die Komplexität dieser Infrastruktur massiv zunimmt und sich die Bedrohungslage täglich weiter zuspitzt, müssen wir uns immer mehr der Tatsache stellen, dass ein erfolgreicher Angriff nicht mehr nur eine Frage der Wahrscheinlichkeit ist. Wir müssen davon ausgehen, dass wir erfolgreich angegriffen werden, oder vielleicht schon erfolgreich angegriffen worden sind.

Um in dieser Realität bestehen zu können, brauchen Unternehmen nicht mehr nur ein klassisches IT Security Team. Erfolgreiche Informationssicherheit benötigt heute das ausbalancierte Zusammenspiel von vielen unterschiedlichen Spezialisten wie technische IT-Spezialisten, Prozessoptimierungs- und Rechtsspezialisten bis hin zu IT Security Architekten, Framework Spezialisten und anderen. Einerseits sind solche Spezialisten äusserst schwer zu finden und andererseits ist es für sehr viele Unternehmen ein Overkill, ein derart grosses und teures Security Team im Hause zu haben. Zudem benötigt man nicht immer die gleichen Spezialisten - je nachdem, was für Projekte gerade im Unternehmen laufen, ändert sich das benötigte Spezialistenwissen.

Die ISPIN AG in Bassersdorf hat sich genau auf diese Problemstellung spezialisiert. ISPIN hat über 15 Jahre Erfahrung im Bereich Cyber Security und verfügt über hochqualifizierte Mitarbeitende. Um Unternehmen das Spezialistenwissen zur Verfügung zu stellen, welches sie je nach Situation benötigen, bietet ISPIN den Security Officer Service an. Bei diesem Service stellt ISPIN einen dedizierten Security Officer zur Verfügung. Dieser übernimmt die Führung der Security im Namen der Unternehmung und setzt Verbesserungsprozesse gemäss Security Masterplan um. Zudem ist er Ansprechpartner für alle internen, security-relevanten Themen. Dieser Security Officer zieht, je nach Bedarf, einen oder mehrere der rund 60 Security-Spezialisten der ISPIN bei und stellt so sicher, dass das richtige Wissen zur richtigen Zeit Vorort ist.

Dass dieses Modell sehr erfolgreich funktioniert, beweist ISPIN täglich bei ihren vielen Kunden, bei denen sie den "Security Officer Service" anbietet. Die Kombination von Flexibilität, personeller Unabhängigkeit und Kostentransparenz in Kombination mit der fachlichen Kompetenz der Security-Spezialisten, welche eine auf den Risikoappetit der Unternehmung abgestimmtes Security-Modell implementieren, überzeugt viele Unternehmen aus der Finanz-, Pharma-, Versicherungs- und Industriebranche, aus dem öffentlichen Bereich und den kritischen Infrastrukturen.

Autor:
Craig Fletcher
Chief Consulting Officer
craig.fletcher@ispin.ch