Mehr Bedrohungen, weniger Experten. Der Fachkräftemangel spitzt sich weiter zu. Wie gehen Sie mit dieser Situation um?

Cyber-Bedrohungen nehmen immer weiter zu, gleiches gilt für den Mangel an Fachkräften für IT-Sicherheit – eine kritische Konstellation für Unternehmen.

Unsere Abhängigkeit von der Technologie, gepaart mit immer raffinierteren und komplexeren Bedrohungen, macht Behörden, Unternehmen und Privatpersonen anfälliger für Cyber-Angriffe. Wenn wir nicht entschlossen dagegen ankämpfen, werden Sicherheitsvorfälle nicht nur zunehmen, sondern auch immer gefährlicher werden und schwieriger zu erkennen sein. Cloudbasierte Services, Mobilgeräte, Big Data und das Internet der Dinge (IoT) greifen immer weiter um sich, sodass vertraute Netzwerkgrenzen verschwimmen. Wir müssen uns daher auf neue Herausforderungen einstellen, um uns umfassend zu schützen. Allerdings wird dies durch einen weltweiten Mangel an Experten für IT-Sicherheit erschwert.

Neue gesetzliche Rahmenbedingungen

Viele Unternehmen verfügen nicht über genügend qualifizierte interne Mitarbeiter, um dieses wachsende Problem im Griff zu behalten und alle Aspekte der Datensicherheit aus eigener Kraft zu bewältigen. Zugleich gehen Bedrohungen nicht mehr nur von einer kleinen Gruppe technisch versierter Hacker aus, da Malware mittlerweile zum Kauf angeboten wird und auch von Cyber-Kriminellen mit wenigen IT-Grundkenntnisse erfolgreich eingesetzt werden kann.

Parallel zur zunehmenden Häufigkeit und Komplexität der Bedrohungen ändern sich die gesetzlichen Rahmenbedingungen und der steigende Bedarf an IT-Sicherheitsexperten rückt ins Zentrum des öffentlichen Bewusstseins. Beispielsweise treten im Mai 2018 mit der EU-Datenschutz-Grundverordnung (EU-DSGVO) neue, strenge Vorgaben in Kraft, die unter anderem hohe Bussgelder für mangelnde Datensicherheit vorsehen. Der deutsche Bundestag hat kürzlich das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) verabschiedet, das die Regelungen der EU-DSGVO umsetzt. In Australien ist mittlerweile der Privacy Amendment (Notifiable Data Breaches) Act 2017 in Kraft getreten, der Unternehmen und Institutionen bei Datenlecks zur Benachrichtigung der Behörden verpflichtet, und in China gilt seit dem 1. Juni 2017 ein neues Cyber-Sicherheitsgesetz. Auch in den USA wird über ein nationales Datenschutzgesetz diskutiert, das Unternehmen dazu verpflichten soll, Datenlecks innerhalb von 30 Tagen zu melden, falls persönliche Daten betroffen sein könnten. Im Risk:Value Report von NTT Security[1] gaben 43 Prozent der Umfrageteilnehmer an, dass gesetzliche Anforderungen und Geldstrafen ihre Hauptmotivation für die Einführung von Datenschutzverfahren sind.

Unternehmenseigene Sicherheitsabteilungen stehen in diesem und den kommenden Jahren vor erheblichen Herausforderungen bei der Rekrutierung neuer Mitarbeiter und sind hinsichtlich der Einhaltung gesetzlicher Vorgaben einer schärferen Kontrolle ausgesetzt.

2015 gaben 62 % der Unternehmen an, über zu wenige interne Sicherheitsexperten zu verfügen, um alle Anforderungen abzudecken. 2017 ist dieser Anteil auf 66 % gestiegen.

Neue Bedrohungen erfordern neue Fähigkeiten

Unternehmen sehen sich ständig mit neuen Sicherheitsbedrohungen konfrontiert. Und da Cyber-Kriminalität mittlerweile ein lukratives Geschäft ist, tauchen jeden Tag neue Herausforderungen und Probleme auf. Gartner prognostiziert, dass bis zum Jahr 2020 weltweit 20,4 Milliarden Geräte mit dem Internet verbunden sein werden[2] – und jedes davon ist ein potenzielles Ziel für Cyber-Angriffe. In ihrem Global Threat Intelligence Report[6] weist die NTT Group darauf hin, dass Unternehmen sich immer noch nicht gegen bekannte Schwachstellen und weniger ausgereifte Bedrohungen schützen – und schon gar nicht gegen neue und ausgeklügelte Angriffsformen.

IT-Teams tun sich schwer damit, auf neue Herausforderungen mit der nötigen Geschwindigkeit zu reagieren, obwohl bei eingehenden Warnhinweisen akuter Handlungsbedarf besteht. Beispielsweise beobachtete NTT Security innerhalb von 24 Stunden nach dem Versand der offiziellen Benachrichtigung über eine Schwachstelle in Apache Struts die

ersten Angriffe mit entsprechenden Exploits. Neue Angriffsmethoden verbreiten sich in der Hacker-Szene schnell. Das erschwert es den ohnehin schon überlasteten IT-Teams zusätzlich, Schritt zu halten und die nötigen Patches rechtzeitig ausfindig zu machen, zu testen und einzuspielen. Angesichts des Trends zur Ausnutzung neuer Schwachstellen, deren Entdeckung nur wenige Tage statt mehrere Jahre zurückliegt, sind präzise Bedrohungsdaten und die Fähigkeit zu raschen Gegenmassnahmen erforderlich. Damit sind die meisten Unternehmen überfordert.

Fachkräftemangel – weltweit

Unterdessen verschärft sich der Fachkräftemangel. Rund um den Globus sind schätzungsweise eine Million Stellen im Bereich IT-Sicherheit unbesetzt, und es ist unwahrscheinlich, dass sich dies in naher Zukunft ändert. Laut der kürzlich veröffentlichten Global Information Security Workforce Studie (GISWS)[3], wird sich die Zahl der unbesetzten Stellen für Cyber-Sicherheitsexperten weltweit im Jahr 2022 auf 1,8 Millionen belaufen. Diese Prognose liegt 20 Prozent über den Schätzungen aus dem Jahr 2015. Von den 19.000 IT-Sicherheitsexperten, die im Rahmen dieser Studie befragt wurden, gaben 66 Prozent an, dass ihr Unternehmen nicht über genügend interne Fachkräfte verfügt, um die immer komplexeren Bedrohungen abzuwehren. (Zum Vergleich: Im Jahr 2015 lag dieser Anteil noch bei 62 Prozent.)

Es fehlt also zunehmend an IT-Sicherheitsexperten, während sich die Bedrohungslage weiter zuspitzt. Als zusätzliche Herausforderung erweist sich auch die rapide Zunahme an neuen Sicherheitstechnologien, -anbietern und -softwarelösungen.

Die Suche nach den richtigen Mitarbeitern

Der Grund für den IT-Fachkräftemangel ist letztendlich unerheblich. Entscheidend ist, dass die Anzahl der Cyber-Angriffe zunimmt. Die Angreifer sind echte Experten, gut organisiert und ausdauernd. In den angegriffenen Unternehmen fehlt es dagegen in der Regel an Wissen und Personal.

Zur Bewältigung dieser Situation sind mehr Mitarbeiter mit dem richtigen Know-how erforderlich. Es sind IT-Fachleute gefragt mit forensischen Kenntnissen, Branchenkenntnissen, Praxiserfahrung im Umgang mit Sicherheitsvorfällen und einem Verständnis der Sicherheitsanforderungen für Mobilgeräte oder Clouds. Darüber hinaus müssen sie mit den aktuellen Compliance-Anforderungen vertraut

IT-Sicherheit – der globale Arbeitsmarkt

- 66 Prozent der Unternehmen verfügen nicht über genügend IT-Sicherheitspersonal.
- 2020 werden im Bereich IT-Sicherheit 1,8 Millionen Fachkräfte fehlen.
- 49 Prozent der global agierenden Unternehmen nennen Schwierigkeiten bei der Rekrutierung qualifizierter Mitarbeiter als wichtigsten Grund für den internen Fachkräftemangel.
- Die Arbeitslosenquote unter den Experten für IT-Sicherheit liegt weltweit bei gerade einmal 2 Prozent.
- 21 Prozent der Fachleute für IT-Sicherheit haben in den Jahren 2016 und 2017 den Job gewechselt.
- Fast 90 Prozent der Fachkräfte für IT-Sicherheit sind Männer.

Global Information Security Workforce Studie (GISWS)[3]

sein. Für diese Positionen kommen auch Fachleute ausserhalb des IT-Bereichs infrage. Die Global Information Security Workforce Studie (GISWS)[3] hat gezeigt, dass 30 Prozent der Befragten vor ihrer Karriere in der IT-Sicherheit in nicht-technischen Geschäftsbereichen wie der Buchhaltung oder dem Marketing tätig waren.

68 % der Unternehmen sind der Meinung, dass zusätzliche Fachkräfte für die Bewältigung der zahlreichen Bedrohungen erforderlich sind.[4]

Ferner sollte die Komplexität moderner IT-Infrastrukturen nicht unterschätzt werden. Ein Unternehmen, dessen IT-Abteilung vielfältige Aufgaben erfüllen muss, benötigt Teams mit einem breiten Spektrum an Skills. Doch viele Unternehmen verfügen nicht über den nötigen Mitarbeiterstamm und erwarten deshalb von ihren IT-Fachkräften, dass sie verschiedene Rollen übernehmen. So ist es zum Beispiel nicht ungewöhnlich, dass ein Windows-Administrator auch für die Einrichtung und Pflege der Firewalls zuständig ist – auch wenn er sich das nötige Know-how lediglich durch die Lektüre eines Schulungshandbuchs angeeignet hat. Das verdeutlicht einmal mehr, dass schlicht nicht genug Fachkräfte für IT-Sicherheit vorhanden sind und dass Unternehmen sich dringend mit ihrer Personalplanung beschäftigen müssen.

Sie haben ein Personalproblem. Was sind Ihre Optionen?

Abwarten

Sie könnten natürlich einfach abwarten und hoffen, dass sich das Problem von selbst löst. Es deutet allerdings nichts auf eine zeitnahe Entspannung auf dem IT-Security-Arbeitsmarkt hin.

Die Häufigkeit und Raffinesse der Internetbedrohungen wird nicht nachlassen, Netzwerke werden immer komplexer und allein die Menge der verfügbaren Daten über Bedrohungen ist eine ständige Herausforderung, wenn nicht genügend Fachkräfte da sind, um aus der Vielzahl Informationen die richtigen Massnahmen abzuleiten.

Die unternehmenseigenen Teams arbeiten jedoch bereits am Limit. Die Global Information Security Workforce Studie (GISWS)[3] weist auf Konfigurationsfehler und Versehen als wesentliche Risikoquellen hin und zeigt auf, dass die Zeit zur Schliessung von Datenlecks nach einem Einbruch in das System kontinuierlich zunimmt. Deshalb ist es beunruhigend, dass die Zahl der Unternehmen mit einem offiziellen Incident-Response-Plan stagniert. Aus dem Risk:Value Report von NTT Security[4] geht hervor, dass 52 Prozent aller Unternehmen weltweit keinen Notfallplan haben und dass dieser Anteil sich in den vergangenen 12 Monaten nicht signifikant verändert hat. Der Mangel an qualifizierten Fachleuten hat also zur Folge, dass es für Unternehmen zunehmend schwieriger wird, mehr zu tun, als nur das Geschäft am Laufen zu halten. Abwarten ist daher keine Lösung.

Die Risiken in Ihrem Unternehmen ermitteln

Bei akutem Fachkräftemangel sollten Sie zunächst Ihre Sicherheitsrisiken ermitteln, bewerten und priorisieren. Auf dieser Grundlage können Sie fundierte Entscheidungen hinsichtlich Ihres Personalbedarfs zur Bekämpfung der Risiken treffen. Ein effektives,

2022 werden weltweit 1,8 Millionen IT-Sicherheitsexperten fehlen – diese aktuelle Prognose liegt 20 % über den Schätzungen aus dem Jahr 2015.

auf die individuellen Geschäftszielen ausgerichtetes Sicherheits- und Risikomanagement ist für jedes Unternehmen wichtig. Oft fehlen aber auch hierfür die Ressourcen. Eine unabhängige Bewertung kann Sie dabei unterstützen, die Risiken für Ihr Unternehmen zu beurteilen, Best Practices abzuwägen, Prioritäten festzulegen und diese im gesamten Unternehmen umzusetzen. Eine solche Analyse kann auch ergeben, dass es wirtschaftlich sinnvoll ist, mehr Fachkräfte einzustellen oder bestimmte Dienstleistungen teilweise oder komplett auszulagern.

Investition in eigene Mitarbeiter

Ihre IT-Abteilung ist bereits mit Ihrer IT-Infrastruktur und Ihren Geschäftsabläufen vertraut und daher bestens auf die Übernahme unternehmensspezifischer Aufgaben im Bereich IT-Sicherheit vorbereitet. Bedenken Sie jedoch, dass der Erwerb und die Vertiefung der erforderlichen Spezialkenntnisse viele Jahre erfordern und daher keine schnelle Lösung für Personalengpässe bieten, sondern vielmehr ein langfristiges Ziel darstellen. Sicherheitsexperten benötigen eine besondere Mischung aus technischem Know-how und Soft Skills: Sie müssen effektiv mit den IT-Laien unter Ihren Mitarbeitern kommunizieren können, sie müssen Ihre Geschäftsprozesse und die gesetzlichen Anforderungen verstehen und sie müssen analytische Fähigkeiten und ein natürliches Interesse an IT-Sicherheit mitbringen.

Die Schulung Ihrer eigenen Mitarbeiter kann langfristig eine lohnende Investition sein, doch IT-Produkte verändern sich schneller, als sich Ihr Team das entsprechende Wissen aneignen kann. Ausserdem erfordert die kontinuierliche Schulung und Weiterbildung eine strategische Entscheidung und ein beträchtliches Budget. Kurzfristig ist sie daher keine zufriedenstellende Lösung.

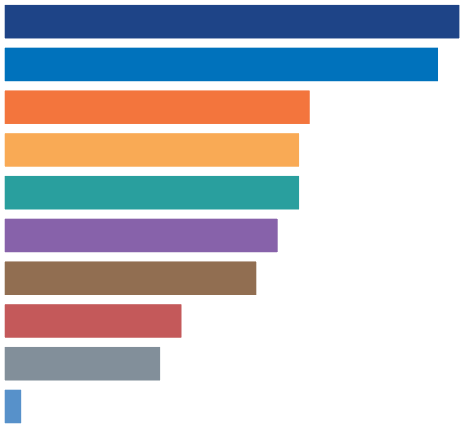
„Wir können den wachsenden Fachkräftemangel in der IT-Sicherheit nicht ignorieren. Deshalb müssen wir die Vorteile des Berufsfelds Cyber-Sicherheit in den Schulen und Universitäten sowie in der gesamten Branche bewerben: die verantwortungsvolle Tätigkeit, die vielversprechenden Karrierechancen, die Arbeitsplatzsicherheit, die gute Bezahlung und die Freude an der Arbeit.“

Garry Sidaway, SVP für den Bereich Security Strategy & Alliances bei NTT Security

Eine angepasste Rekrutierungsstrategie

Ein kürzlich veröffentlichter Bericht nennt verschiedene Bereiche, in denen Unternehmen ihre Rekrutierungsstrategien verbessern und dadurch die für 2022 prognostizierte Personallücke von 1,8 Millionen Fachkräften zumindest teilweise schliessen könnten.

Abbildung 1 Gründe für die Auslagerung an externe Anbieter



43% Für die Datenspeicherung
41% Um Unterstützung beim Datenmanagement zu erhalten
29% Um Zugang zu besseren Technologien zu erhalten
28% Weil unsere internen Ressourcen nicht ausreichen
28% Weil unsere internen Kenntnisse und Fähigkeiten nicht ausreichen
26% Weil wir bestimmte Geschäftsprozesse auslagern (z. B. im Personalwesen, bei der Lohnabrechnung, bei der Bearbeitung von Vertriebsaufträgen, in der Finanzabteilung usw.)
24% Weil es billiger ist, das auszulagern
17% Weil wir Unterstützung bei der Migration in die Cloud benötigen
15% Weil wir Unterstützung bei der Aktualisierung unserer Systeme benötigen
2% Ich weiss es nicht

Risk:Value Report von NTT Security[4]

Zum einen ist der Bereich IT-Sicherheit grösstenteils eine männliche Domäne – nur 11 Prozent der weltweiten Fachkräfte sind Frauen[5]. Diese werden im Vergleich zu ihren männlichen Kollegen deutlich häufiger diskriminiert und ausserdem schlechter bezahlt, obwohl sie beim Einstieg üblicherweise höher qualifiziert sind. Es muss also auf allen Ebenen mehr getan werden, um Frauen dazu zu ermutigen, die IT-Sicherheit als ein mögliches Berufsfeld in Betracht zu ziehen. Wir müssen dafür sorgen, dass in den Schulen und Universitäten eine entsprechende Berufsberatung stattfindet. Zum anderen geht aus dem Bericht hervor, dass knapp ein Drittel der erfolgreichen Sicherheitsexperten ihre Karriere in einem nicht-technischen Bereich bzw. mit einer nicht-technischen Ausbildung beginnen.

„Der grosse Vorteil bei Managed Services ist, dass die Anbieter oft einen besseren Überblick über das weltweite Geschehen haben, im Unterschied zum internen Team, das nur das eigene Netzwerk im Blick hat.“

Dark Reading (Magazin für Internetsicherheit)

Mitarbeiter, die über Kommunikationstalent und geschäftliches Know-how verfügen, können einen wichtigen Beitrag zur IT-Sicherheit leisten. Die Fähigkeit zuzuhören, sich in andere hineinzuversetzen und Cyber-Sicherheit verständlich zu machen, ist eine der Grundvoraussetzungen dafür, dass Unternehmen fundierte Entscheidungen treffen können. Personalmanager sollten das bei der Rekrutierung berücksichtigen.

Zugleich ist zu beobachten, dass Mitarbeiter aus der Generation der Millennials materielle Anreize tendenziell niedriger gewichten als ihre älteren Kollegen.

Das zwingt Personalabteilungen dazu, ihre aktuellen Rekrutierungsstrategien zu überdenken, die Einstellung von Experten aus verschiedenen Bereichen in Erwägung zu ziehen und sich ein genaueres Bild davon zu machen, was die Mitarbeiter ihres Unternehmens motiviert. Derzeit sind die Erwartungen der Personalmanager an neue Mitarbeiter nicht deckungsgleich mit den Voraussetzungen für eine erfolgreiche Karriere. Der weltweite Mangel an Fachkräften wird erst abnehmen, wenn sich diese Schere schliesst.

Investition in externe Mitarbeiter

Der Aufbau und das Management eines eigenen Teams von IT-Sicherheitsexperten bringen etliche Herausforderungen mit sich. Zunächst einmal kostet es Zeit und Geld, bis für jede Position die passende Person gefunden ist. Zudem sind regelmässige Weiterbildungsmassnahmen erforderlich, damit der Wissensstand im Team aktuell bleibt. Und wenn jemand das Unternehmen verlässt, müssen Sie wieder von vorn anfangen. Der kürzlich von NTT Security veröffentlichte Risk:Value Report[4] nennt neben dem Mangel an unternehmensintern verfügbaren Skills und Ressourcen eine Reihe weiterer Gründe für die Inanspruchnahme von Managed Security Services externer Anbieter (siehe Abbildung 1).

„Ermitteln Sie, welche Sicherheitsprozesse (wie beispielsweise das Log-Management) stark routinemässig ablaufen und von Drittanbietern übernommen werden können. Viele Unternehmen mit begrenzten Ressourcen bewältigen die Herausforderungen der IT-Sicherheit, indem sie auf Managed Security Services zurückgreifen.“

John Petrie, CISO von NTT Security

Die Auslagerung von Sicherheitsdienstleistungen

Durch die teilweise oder vollständige Auslagerung Ihrer IT-Sicherheit an einen professionellen Anbieter von Sicherheitsdienstleistungen können Sie diesen Mangel ausgleichen. Diese Anbieter wissen, wie und wo sie die richtigen Fachkräfte für Ihre Branche finden, und investieren in die Aus- und Weiterbildung qualifizierter Spezialisten. Sie überwachen Ihr Netzwerk Tag für Tag rund um die Uhr und nehmen Ihren Mitarbeitern zeitraubende Routineaufgaben ab.

Managed Security Services ist eine Branche in stetigem Wandel. Die Zusammenarbeit mit einem professionellen Sicherheitsdienstleister kann auf jeden beliebigen Service beschränkt werden, für den Sie intern nicht die geeigneten Mitarbeiter finden, z. B. die Risikoanalyse, die Erstellung eines Incident-Response-Plans oder die Betreuung eines Projekts zur Umsetzung gesetzlicher Vorschriften. Alternativ entscheiden sich viele Unternehmen dafür, ihre IT-Sicherheit komplett an einen auf diesen Bereich spezialisierten Anbieter auszulagern.

Bei der vollständigen Auslagerung geht es nicht mehr nur darum, komplexe Netzwerke am Laufen zu halten, sondern darum, Ihr Unternehmen rund um die Uhr vorausblickend gegen vielfältige und komplexe Angriffe zu schützen und über die reine Geräteverwaltung hinaus ergänzende Informationen und Analysen zu liefern. Bei einer Entscheidung für einen globalen Anbieter profitieren Sie nicht nur von der grossen Erfahrung lokaler Mitarbeiter, sondern von weltweiten Expertenpools und Systemen Ihres Anbieters.

Anbieter von Sicherheitsdienstleistungen sind immer über aktuelle und neuartige Bedrohungen und Schwachstellen auf dem Laufenden und haben Zugriff auf Informationen über regionale und globale Bedrohungen. Mit ihrer Unterstützung können Sie Bedrohungen frühzeitig begegnen und den Angreifern einen Schritt voraus bleiben, anstatt erst zu reagieren, wenn es zu spät ist. Der richtige Anbieter kann das Management äusserst komplexer Infrastrukturen und verschiedenster Anwendungen übernehmen, unabhängig davon, ob diese in Ihrem Rechenzentrum, in der Cloud oder in einer Hybrid-Umgebung implementiert sind.

Fazit

Die Bedrohungslage ändert sich zu schnell, als dass Unternehmen Schritt halten könnten. Die zunehmende Nutzung von Cloud-Services, Mobilgeräten, Big Data und dem Internet der Dinge verschärft die Situation zusätzlich. Unternehmen verfügen schlicht nicht über genug IT-Sicherheitsexperten und die Schulung der eigenen oder Einstellung neuer Mitarbeiter lösen das Problem auf kurze Sicht nicht. IT-Sicherheit muss als Karriereoption in das öffentliche Bewusstsein rücken und Schulen und Universitäten weltweit müssen die Problematik thematisieren, um mehr junge Menschen für diesen Beruf zu interessieren. Bis dahin müssen Unternehmen sorgfältig abwägen, ob sie in Zukunft mit ihren vorhandenen Ressourcen improvisieren oder ihren Sicherheitsbetrieb ganz oder teilweise an einen vertrauenswürdigen externen Anbieter auslagern wollen. Diese Entscheidung war noch nie von so weitreichender Bedeutung wie heute.

Über NTT Security

NTT Security ist das auf Informationssicherheit und Risikomanagement spezialisierte Unternehmen der NTT Group (Nippon Telegraph and Telephone Corporation), einem der grössten IKT-Unternehmen weltweit. Der Experte für IT-Security steht für ein ganzheitliches Sicherheitskonzept und die Bereitstellung ausfallsicherer Lösungen, die den Anforderungen der Kunden vor dem Hintergrund des digitalen Wandels gerecht werden. Mit zehn globalen SOCs, sieben Zentren für Forschung und Entwicklung sowie mehr als 1.500 Sicherheitsexperten unterstützt NTT Security Unternehmen auf sechs Kontinenten bei der Reaktion auf Hunderttausende Sicherheitsvorfälle pro Jahr.

NTT Security bietet Kunden die richtige Mischung aus Beratung, Managed Services und Technologien, indem lokales Know-how optimal mit globalen Ressourcen kombiniert wird. Weitere Informationen finden sich unter **nttsecurity.com/ch**.

1. Risk:Value Report 2016, NTT Security 2. Pressemitteilung von Gartner 3. Global Information Security Workforce Study (GISWS), Frost & Sullivan mit Unterstützung von (ISC)², Booz Allen Hamilton und Alta Associates für das Center for Cyber Safety and Education 4. Risk:Value Report 2017, NTT Security 5. Whitepaper “The 2017 Global Information Security Workforce Study: Women in Cybersecurity”, Frost & Sullivan 6. Global Threat Intelligence Report 2016, NTT Security