WHITEPAPER

10 Maßnahmen für proaktive Cybersicherheit

solarwinds msp

Dass die digitale Gefahrenlage ständig im Wandel ist, dürfte inzwischen jedem bekannt sein, schließlich lassen sich kriminelle Hacker immer neue Angriffsmaschen einfallen. Dabei sind die Hacker nicht das einzige Problem, denn auch das Risiko, dass arglose Systembenutzer versehentlich eine Datenpanne auslösen, steigt angesichts der immer stärkeren Digitalisierung unserer Welt mehr denn je.

Wie ernst die Lage inzwischen ist, zeigt ein kurzer Blick auf die Daten-Skandale des Jahres 2017: Gut 143 Millionen sensibler Datensätze wurden bei einem Einbruch in die Systeme der US-amerikanischen Bonitätsauskunftei Equifax® erbeutet[1]. Wenn schon ein Unternehmen, das sich selbst strengste Geheimhaltung auf die Fahnen schreibt, Mühe mit dem Datenschutz hat, um wie viel schwieriger mag es dann für ein durchschnittliches Unternehmen sein. Mit Ransomware-Schädlingen wie Petya, WannaCry und Bad Rabbit müssen die Bösewichte, um ihr Ziel zu erreichen, nicht einmal mehr Datensätze stehlen; es reicht schon, den Zugriff darauf zu vereiteln und das Opfer derart in Bedrängnis zu bringen, dass es für die Freigabe der Daten zu zahlen bereit ist.

Was nottut, ist ein Paradigmenwechsel in der Sicherheit, der die gesamte Branche in die Lage versetzt, Internetverbrecher proaktiver zu bekämpfen. Mit welchen 10 Maßnahmen dies gelingen kann, lesen Sie in diesem Whitepaper.

Was nottut, ist ein Paradigmenwechsel in der Sicherheit, der die gesamte Branche in die Lage versetzt, Internetverbrecher proaktiver zu bekämpfen.

1. ÜBER RISIKEN REDEN, NICHT ÜBER SICHERHEIT

Kein Unternehmen ist hundertprozentig sicher, da mag es noch so gute Technik haben. Ein Risiko, zum Opfer der allerneuesten Angriffsmasche zu werden, bleibt immer bestehen. Nichtsdestotrotz geht es vielfach noch zu stark um die Frage, ob ein System „sicher ist" oder eben nicht. Dieses Schwarzweiß-Denken geht an der Realität komplett vorbei.

Sprechen Sie mit Kunden also lieber über Risiken anstatt über Sicherheit. Bei „Risiken" denken die meisten Unternehmen an generelle Desaster wie eine negative Publicity oder Markteinbrüche – weniger an Cybersicherheit. Beherzigen Sie darum die folgenden Tipps:

» **Mit dem Kunden das Ausmaß des Risikos abschätzen:** Statt gleich über Sicherheitsmaßnahmen zu reden, ermitteln Sie lieber als Erstes, welchen Imageschaden Ihr Kunde von einem Verlust oder Diebstahl seiner Daten davontrüge. Bei einer großen Bonitätsauskunftei wie Equifax ist dieser Schaden selbstverständlich enorm. Doch auch kleine Unternehmen kommen bei Verlust von Kundendaten schnell in schwierige Fahrwasser. Eigentlich müssen sich die Kleinen

noch viel mehr Sorgen machen als die Großen, da ihre Systeme im Schnitt einfacher zu hacken sind (insbesondere mit automatisierten Angriffsmethoden). Außerdem fehlt ihnen oft das finanzielle Polster, um die Konsequenzen einer Datenpanne abzufedern. Wenn Sie also mögliche Risiken ansprechen, kann Ihr Kunde definitiv erkennen, was auf dem Spiel steht, und wird das Thema Sicherheit zukünftig sicherlich ernster nehmen.

- **Kennzahlen einsetzen – und sie mit Argusaugen überwachen:** Kennzahlen belegen dem Kunden gegenüber nicht nur den Wert Ihrer Sicherheitsleistungen, sondern halten Sie über den Sicherheitszustand von Systemen und verbesserungswürdige Bereiche auf dem Laufenden. Wenn Sie zum Beispiel ermitteln können, bei wie vielen Programmen noch die neuesten Sicherheitspatches fehlen, dann weist dieser Prozentwert Sie auf potenzielle Sicherheitslücken hin. Exakt diese Kennzahl hätte den Equifax-Datenklau und auch WannaCry verhindern können: In beiden Fällen hatten die Angreifer Schlupflöcher genutzt, für deren Schließung schon Monate zuvor Patches freigegeben worden waren[2,3].
- **Tadelloses Management = lückenlose Sicherheit:** Indem Kennzahlen Ihnen Schwachstellen aufzeigen, helfen sie Ihnen dabei, Prozesse zu optimieren. „Nur was sich messen lässt, lässt sich managen", heißt es bekanntlich. Können Sie beispielsweise messen, wie schnell Ihre Techniker auf Sicherheitsvorfälle reagieren, dann erfahren Sie, ob hier vielleicht Optimierungspotenzial besteht. Und können so peu à peu Ihren Kundenservice verbessern.

2. DIE „KRONJUWELEN“ BEWACHEN

Etliche Kinofilme oder Fernsehserien handeln davon, wie Schurken ein „großes Ding drehen“ – einen Einbruch, Raub oder Überfall. In Ocean’s 11[4] zum Beispiel sollen gleich drei Casinos ausgeraubt werden. In anderen Filmen sind es Banken, in der sechsten Folge der BBC-Serie „Sherlock“[5] raubt Bösewicht Moriarty gar die britischen Kronjuwelen (und lässt sich dafür absichtlich verhaften).

Im Film betreiben die Beraubten ihren unglaublichen Sicherheitsaufwand letztlich immer vergeblich. Lassen Sie sich davon nicht beirren: Sie müssen wissen, wo sich die „Kronjuwelen“ in der IT-Umgebung Ihres Kunden befinden. Dann können Sie den realen Moriartys da draußen durchaus die Stirn bieten.

Für Schutz und Wartung von Servern und Endgeräten haben Sie ja sicherlich ein Konzept; jetzt müssen Sie noch überlegen, wo darin genau die Preziosen – Daten nämlich – lagern. Als IT-Serviceanbieter Ihres Kunden kennen Sie seine Systeme wie die eigene Westentasche. Das macht es leichter, sie einmal aus der Perspektive der bösen Buben zu betrachten.

Als Erstes suchen Sie also, wie bereits gesagt, unter den Anwendungen, Systemen und Daten nach den Kronjuwelen. Auch manche Mitarbeiter beim Kunden können „Preziosen“ sein, die mit speziellen Prozessen besonders geschützt werden sollten.

Auf ganz bestimmte Unternehmensangehörige zielende Angriffe können verheerende Folgen haben: Sie müssen sich nur vorstellen, einem Finanzchef werden vom Laptop Daten gestohlen – der GAU für sein Unternehmen …

Zu den Kronjuwelen können auch bestimmte Prozesse oder Zugangspunkte gehören. Im Fall der US-amerikanischen Handelskette Target® hackten sich die Datendiebe ins Unternehmensnetzwerk, indem sie eine Sicherheitslücke in den Systemen eines Dienstleisters für Heizung und Klima ausnutzten[6].

Zuweilen sind es auch bestimmte Daten, die besonders abgesichert werden müssen. Krankenakten zum Beispiel enthalten eine Vielzahl hochsensibler Daten, die für Online-Ganoven lukrative Beute darstellen. Ebenfalls sehr begehrt sind Kreditkartendaten.

Erster Punkt, wie gesagt: die Kronjuwelen des Unternehmens bestimmen und diese entsprechend streng absichern. Wichtig ist es außerdem, regelmäßig zu prüfen, ob die eigenen Sicherheitsrichtlinien eine ausreichende Sicherheit der betreffenden Ressourcen – Personen, Systeme, Zugangspunkte oder Daten – gewährleisten können. Alles abzusichern ist quasi unmöglich; auf die Kronjuwelen jedoch sollten Sie als Anbieter von Sicherheitskonzepten prinzipiell immer ein Auge haben.

3. AUF „CYBERHYGIENE“ ACHTEN

Bei den Maßnahmen 1 und 2 geht es darum, mögliche Risiken stärker ins Blickfeld des Kunden zu rücken. Davon abgesehen gelten die Grundregeln der Cybersicherheit: Nur mit guter Technik, geeigneten Prozessen und dem richtigen Aufwand optimieren Sie den Schutz und senken das Risiko.

Sie müssen, mit anderen Worten, Cyberhygiene betreiben. Wenn Sie kontinuierlich auf der Hut vor Angreifern sind, können Sie sich selbst und Ihren Kunden viel Unbill ersparen: Nach wie vor sind es häufig die simplen Tricks, die Erfolg haben: Phishing-E-Mails oder verseuchte E-Mail-Anhänge.

Im Rahmen einer guten Cyberhygiene müssen Sie …

- **… auf allen Endgeräten im System wirksamen Virenschutz installieren und engmaschig Virenscans durchführen,**
- **… die Datenlandkarte des betreuten Systems kennen, um unbefugte Zugriffe erfolgreich verhindern zu können,**
- **… Administrator- und Benutzerrechte für den Zugriff auf sensible Daten engmaschig prüfen,**
- **… Systeme und Software regelmäßig patchen (und auf Sicherheitsempfehlungen und -bulletins achten),**
- **… einen funktionierenden Backup- und Business-Continuity-Plan aufstellen,**
- **… vor Spam auf der Hut sein und Mailserver für seine Abwehr technisch ausrüsten,**
- **… die Angriffsfläche verkleinern – durch Abkopplung wichtiger Systeme vom Internet oder Verwendung virtueller Maschinen, wo möglich,**
- **… die Vorfallreaktion und Behebungsroutinen planen, um für den Ernstfall klare Handlungsabläufe zu haben.**

Letztlich gilt: Die Wunderwaffe schlechthin gibt es nicht; es geht vielmehr darum, ständig auf der Hut zu sein und kontinuierlich bei der Stange zu bleiben. Für Sie als MSP ist das eine gute Nachricht: Der Service, den Sie bieten, ist für Ihre Kunden von hohem Wert und Ihnen selbst verschafft er wiederkehrende Umsätze.

4. DIE UMGEBUNG AUF MEHREREN EBENEN SCHÜTZEN

Kein System lässt sich hundertprozentig abdichten, und ein Sicherheitskonzept, das für alles und jeden passt, gibt es auch nicht.

Deshalb sollten Sie stets gut überlegen, wie viel Aufwand sich für die Absicherung eines von Ihnen betreuten Systems lohnt. Schießen Sie mit Kanonen auf Spatzen, so wird Ihr Kunde angesichts der hohen Kosten, die entstehen, vielleicht skeptisch, ob dieser Aufwand denn nötig ist. Sind Sie hingegen zu sparsam, so steigt sein Risiko, Opfer eines Hackerangriffs zu werden.

Entscheiden Sie also von Fall zu Fall, denn jeder Kunde hat bekanntlich andere Kronjuwelen. Kennen Sie diese, können Sie das jeweils optimale Schutzniveau leichter bestimmen. Wichtig ist, dass Sie den Kunden von Anbeginn in Ihre Überlegungen einbinden, um zu erfahren, was man von Ihnen erwartet, und so den besten Lösungsweg zu finden.

Im Zuge Ihrer Systembetreuung sollten Sie den betreffenden Kunden regelmäßig auf dem Laufenden halten und ihm immer wieder darlegen, was genau er von den Leistungen hat, die Sie für ihn erbringen. Damit signalisieren Sie ihm, dass seine Systeme bei Ihnen in den besten Händen sind. Im Viertel- bis Halbjahresturnus sollten Sie das aktuelle Schutzniveau der Umgebung auf den Prüfstand stellen, damit sie gegen potenzielle neue Gefahren immer gut gewappnet ist. Bedenken Sie, dass die Bedrohungen sich ständig wandeln – hier müssen Sie als MSP immer Schritt halten. Ransomware zum Beispiel war vor ein paar Jahren noch gar kein Thema, gehört aber leider inzwischen zu den beliebtesten Angriffsmaschen.

5. SICHERHEIT ALS WETTBEWERBSFAKTOR NUTZEN

Gefahren wird es immer geben. Da wird Sicherheit zum wettbewerbsentscheidenden Faktor – für Sie und für Ihre Kunden.

Für Ihr eigenes Geschäft liegen die Vorteile auf der Hand: Mit einem Rundumservice für Sicherheit heben Sie sich von Konkurrenten ab, die auf simple Überwachungs- und Wartungsangebote setzen. Sie können die Nachfrage nach ganzheitlichen Schutzkonzepten decken und positionieren sich als kompetenter Anbieter.

Welchen Wettbewerbsvorteil Ihr Kunde durch Sicherheit hat, mag auf den ersten Blick weniger offensichtlich sein. Aber angenommen, einer Ihrer Kunden würde für staatliche Versorgungsunternehmen arbeiten und könnte diesen ein hohes Sicherheitsniveau seiner Systeme garantieren, dann könnte ihm das sehr wohl mehr Geschäft bescheren. Einige Ihrer Kunden gehören vielleicht Branchen an, in denen Sicherheit unabdingbar ist; sie sind möglicherweise Banken, Krankenhäuser, Pharmaunternehmen, Vertragspartner staatlicher Geheimdienste oder Versorgungsunternehmen. Wenn diese Kunden belegen können, dass ihre Systeme mit modernster Sicherheitstechnik geschützt und kontinuierlich überwacht werden, dann ist das ohne Frage ein Marktvorteil für sie.

Doch auch Unternehmen aus weniger stark regulierten Branchen nutzt das Alleinstellungsmerkmal „Sicherheit“, auch wenn ihnen das vielleicht gar nicht bewusst ist. Ein Hersteller für digitale Heizungstechnik zum Beispiel könnte Opfer eines Angriffs werden, bei dem die Hacker über smarte Thermostate in seine Systeme eindringen, wie es White-Hat-Hacker auf der Def Con 2016 demonstriert haben[7]. Derlei Angriffe gab es zwar bislang noch nicht, aber Ihr Kunde könnte zeigen, dass er im Fall der Fälle gewappnet wäre. Fest steht: IoT-Geräte stellen ein Risiko für Unternehmen dar. Der Umstand, dass ein Unternehmen mit einem professionellen Dienstleister für IT-Sicherheit zusammenarbeiten, wie Sie es sind, hebt es von seiner Konkurrenz ab.

Im Viertel- bis Halbjahresturnus sollten Sie das aktuelle Schutzniveau der Umgebung auf den Prüfstand stellen, damit sie gegen potenzielle neue Gefahren immer gut gewappnet ist.

6. VORSCHRIFTEN ALS CHANCEN BEGREIFEN

Wenn ein neues Gesetz in Kraft tritt – so wie diesen Mai die EU-Datenschutz-Grundverordnung (DSGVO) –, tun sich die IT-Branche und ihre Fachpresse häufig erst einmal schwer damit, seine Auswirkungen abzuschätzen. Dann machen sich Verunsicherung und Panik breit.

Dabei liegen in jeder Gesetzesneuerung, von ihrem eigentlichen Zweck abgesehen, Chancen, die Sie als wettbewerbsbewusster MSP durchaus für sich nutzen können. Machen Sie sich Folgendes klar:

- **Regulierung fördert die Sicherheit:** Die DSGVO oder andere Datenschutzgesetze wie etwa das US-amerikanische HIPAA-Gesetz zwingen Unternehmen dazu, ihre Sicherheit zu verbessern. Die Gesetze bringen aber nicht nur Ihre Kunden dazu, Sicherheit ernst zu nehmen. Sie selbst erhalten durch sie eine Orientierungshilfe für das erfolgreiche Schließen von Sicherheitslücken – über den Gesetzestext selbst sowie den Diskurs, der sich dazu in der Fachpresse entwickelt.
- **Behalten Sie die Gesetze im Auge, die für potenzielle Kunden gelten:** Operiert ein Unternehmen in einer bestimmten Weltregion, so unterliegt es den dort gültigen Gesetzen. Ein Beispiel dafür ist die Regelung des Umgangs mit persönlichen Daten von EU-Bürgern durch die DSGVO. Manche Unternehmen gehören stark regulierten Branchen an: Finanzen, Gesundheitswesen, Bildungswesen, öffentliche Hand. Wer auch immer Ihre Kunden sind, eine Rechtsberatung sollten Sie für jeden Einzelfall einholen, um Ihre Verträge haftungssicher zu gestalten. Darüber hinaus gilt: Um Ihre Kunden adäquat schützen zu können, müssen Sie sich zur geltenden Gesetzeslage stets auf dem neuesten Stand halten.
- **Der Umgang mit persönlichen Daten wird immer stärker reguliert:** Mit der DSGVO ergibt sich ein deutlich umfassenderer Anwendungsbereich für Datenschutz-Regelungen, denn sie gilt auch für Unternehmen mit Sitz außerhalb der EU, wenn diese in Kontakt mit persönlichen Daten von EU-Bürgern kommen. Die allgemeine Stoßrichtung lässt sich an der aktuellen Entwicklung sicherlich ablesen: 1. Ausweitung des Anwendungsbereichs und 2. immer stärkerer Schutz für persönliche Daten.

Vorschriften in puncto Sicherheit sollten Sie wirklich als Chance begreifen. Sie verbessern die Sicherheit nicht nur in einzelnen Unternehmen, sondern insgesamt – und genau Letzteres ist angesichts der durchgängigen digitalen Vernetzung unserer Welt sehr wichtig. Den MSPs wiederum bieten sich damit Geschäftschancen bei Kunden aus stark regulierten Branchen, die häufig besonders lukrativ sind.

7. SICHERHEITSKENNTNISSE AUSBAUEN

Die Cybersicherheit ist ständig im Wandel, wie bereits gesagt. Waren vor noch nicht allzu langer Zeit Backups im eigenen Rechenzentrum im Ernstfall völlig ausreichend, so ist eine Zweitkopie in der Cloud heute schon fast Pflicht, denn es gibt inzwischen Malware, die es speziell auf Backup-Dateien abgesehen hat.

Die eigenen Kenntnisse zum Thema Sicherheit immer aktuell zu halten, ist wichtig – für Ihre Kunden sowie für die IT-Branche insgesamt. Unsere Tipps zum Thema Wissensaufbau:

Die eigenen Kenntnisse zum Thema Sicherheit immer aktuell zu halten, ist wichtig – für Ihre Kunden sowie für die IT-Branche insgesamt.

- **Wissensfundus im eigenen Betrieb organisieren:** Als Erstes sollten Sie sicherstellen, dass Ihr Unternehmen vom Wissen und den Fähigkeiten her in der Lage ist, kompetente Unterstützung zu leisten. Jeder Ihrer Mitarbeiter sollte mit den Grundlagen der Systemüberwachung und der Cyberhygiene vertraut sein. Im Zuge der Arbeit mit verschiedenen Kunden bilden sich u. U. Zuständigkeiten mancher Mitarbeiter für einen bestimmten Kunden heraus. Diese Mitarbeiter kennen dann die Schwachpunkte im System dieses Kunden besonders gut, weshalb ihr Know-how in einem Ernstfall entscheidend sein kann. Achten Sie deshalb darauf, dass Ihre Spezialisten alles, was sie zu einem bestimmten System wissen, zentral zugänglich, zum Beispiel auch beim Helpdesk, ablegen, sodass andere im Betrieb notfalls darauf zugreifen können.
- **Aktuelle Entwicklungen verfolgen:** Um hochkarätigen Service bieten zu können, sollten Sie regelmäßig viel lesen und recherchieren, zum Beispiel die aktuellen Tagesmeldungen der großen Fachportale. Ergänzend können Sie ggf. Newsletter oder Blogs von Infodiensten abonnieren, die Ihnen besonders zusagen. Hier ein paar Empfehlungen:
  - United States Computer Emergency Readiness Team: https://www.us-cert.gov
  - SANS.org (mit Newslettern und Blogs): https://www.sans.org
  - Cloud Security Alliance: https://cloudsecurityalliance.org
  - ZDnet: http://www.zdnet.com
  - Dark Reading: https://www.darkreading.com
  - CSO Magazine: https://www.csoonline.com
- **Zertifikate erwerben:** Zertifizierungen helfen Ihren Technikern, fachlich auf dem neuesten Stand zu bleiben, und bieten einen Orientierungsrahmen bei der Bekämpfung der Cyberkriminalität. Mit Zertifikaten unterstreichen Sie Ihre Kompetenz und Seriosität; sie nutzen also auch Ihrem Marketing. Empfehlenswert

sind das CISSP-Zertifikat (Certified Information Security Services Professional), das CEH-Zertifikat (Certified Ethical Hacker) oder das (ISC-)2-Zertifikat (International Information System Security Certificate Consortium).

» **Sich in der eigenen Fachwelt vernetzen:** Hilfreich ist auch der Kontakt und Austausch mit Fachkollegen mit Schwerpunkt Sicherheit. Auch ein Beitritt zur ISACA, dem Berufsverband für IT-Revision und -Governance und Informationssicherheit, kann sinnvoll sein. Ergänzend sollten Sie Fachkonferenzen besuchen, die in allen Weltregionen regelmäßig abgehalten werden, etwa die RSA Conference, die Black Hat Conference, die Def Con, die Cloud Security Expo und Cybersecurity Europe, um nur ein paar zu nennen.

8. EINE SICHERHEITSKULTUR ENTWICKELN

Sicherheit muss zum Kern eines jeden Unternehmens zählen. So hilfreich Technik sein mag, sie hat ihre Grenzen. Mit täglich neuen Malware-Varianten, kriminellen Websites und erschreckend echt wirkenden Phishing-Mails wird die Technik nie vollständig mitkommen.

Sind Sie innerhalb der Sicherheitsbranche gut vernetzt, so haben Sie es im Kampf gegen Kriminelle leichter.

Schulen Sie also Ihre Kunden (und auch Ihr eigenes Personal) zum Thema Sicherheit – und zwar regelmäßig. Alle müssen vernünftige Sicherheitspraktiken erlernen – Kennwörter häufig ändern, verschiedene Kennwörter nutzen (was mit einem Kennwortspeicher komfortabel ist), Mobilgeräte verschlüsseln usw. – und diese zur Sicherheit des eigenen Unternehmens beherzigen. Mit „regelmäßig" meinen wir genau das – regelmäßig. Eine Unterweisung genügt sicher nicht. Machen Sie so oft wie möglich Auffrischungsangebote.

Gleichfalls wichtig: Informieren Sie die Systembenutzer Ihres Kunden unmittelbar, wenn neue Bedrohungen im Umlauf sind. Der Angriff auf Google® Docs 2017 lief beispielsweise über eine Phishing-E-Mail. Sie lockte ahnungslose Empfänger unter Eingabe ihrer Google-Anmeldedaten auf eine Fake-Website, von der aus die Hacker sich Zugriff auf das Konto und die Adressbücher der Betreffenden verschafften und dieselbe Masche bei seinen Kontakten fortsetzten. Eine schlichte Mitteilung an Ihre Kunden, dass diese eine E-Mail mit einem bestimmten Betreff oder Inhalt lieber nicht öffnen sollten, kann Ihnen viel Kummer ersparen.

9. SICHERHEIT ALS TÜRÖFFNER IM VERKAUFSGESPRÄCH NUTZEN

Digitale Sicherheit wird immer relevant bleiben, solange es digitale Systeme gibt. Wenn es Ihnen gelingt, Ihr Unternehmen als kompetenten Sicherheitspartner zu positionieren (der stets auf dem aktuellen Stand des Geschehens ist, wie unter Punkt 7 beschrieben), werden sich Ihnen immer wieder Geschäftschancen eröffnen.

Sicherheit kann ein Aufhänger für das Anbieten weiterer Services sein. In einem Verkaufsgespräch zur mehrschichtigen Sicherheit könnten Sie dem Kunden beispielsweise erläutern, welchen Nutzen er diesbezüglich von einer rundum tadellos gemanagten Umgebung hätte. Wie steht es mit der Netzwerkperformance? Was ist mit dem Backup wichtiger Daten? Sie müssen im Gespräch nicht beim ursprünglichen Thema „Sicherheit" bleiben, sondern können Ihren Kunden ruhig fragen, welche weiteren Services er noch brauchen könnte.

10. ALLIANZEN SCHMIEDEN

Kriminelle Hacker bewegen sich in ihren eigenen Communitys und lernen ihr Handwerk von Gleichgesinnten.

Auch Sie sollten Allianzen schmieden: Ob Sie nun Fachverbänden beitreten, Konferenzen besuchen, die Fachpresse lesen oder wichtige Erkenntnisse teilen: Sind Sie innerhalb der Sicherheitsbranche gut vernetzt, so haben Sie es im Kampf gegen die Bösewichte leichter.

Beschränken Sie sich dabei keineswegs auf die Fachwelt der Cybersicherheit, sondern nutzen Sie jede Gelegenheit, sich mit anderen Vertretern der IT-Branche zu treffen und auszutauschen. In einer Verkaufsschulung können Sie beispielsweise lernen, wie Sie Sicherheitsdienstleistungen besser positionieren oder das Thema Risiko besser platzieren und daraus vielleicht Kapital schlagen können.

Fest steht: Sie sind im Kampf gegen Cyberschurken nicht auf sich gestellt.

CHANCEN FÜR IHR GESCHÄFT

Die sich im Umbruch befindliche Sicherheitslage bedeutet jede Menge Geschäftschancen für Ihr Unternehmen, wie unsere eigenen Untersuchungen dazu zeigen.

Erst kürzlich ergab eine unserer Umfragen unter 400 US-amerikanischen und britischen Unternehmen: 80 % der Unternehmen haben vor, ihren Umgang mit dem Thema Sicherheit in den nächsten 12 Monaten zu ändern. Und von denen, die sich bislang selbst um ihre Sicherheit gekümmert haben, möchten 82 % in den nächsten 12 Monaten mindestens einen Teil dieses Bereichs auslagern[8].

Diese Zahlen sagen klipp und klar: MSPs, die Sicherheitsleistungen anbieten, haben jede Menge neuer Geschäftschancen, und dieser Markt wird in absehbarer Zeit auch nicht verschwinden, denn die digitalen Bedrohungen werden bleiben.

Beherzigen Sie einfach die Tipps dieses Whitepapers: Sprechen Sie über Risiken, überlegen Sie, welcher Schutzaufwand angemessen ist, betreiben Sie vernünftige Cyberhygiene und informieren Sie sich regelmäßig zu aktuellen Entwicklungen. All dies wird dazu führen, dass Sie im Kampf gegen die Internetkriminalität die Oberhand behalten. Was Ihnen Ihre Kunden danken werden.

REFERENZEN

[1,2] „Equifax Officially Has No Excuse“; Wired. https://www.wired.com/story/equifax-breach-no-excuse (Aufruf im Dezember 2017).

[3] „The ‚WannaCry“ Ransomware Attack Could Have Been Prevented. Here’s What Businesses Need to Know“; CNBC. https://www.cnbc.com/2017/05/17/the-wannacry-ransomware-attack-what-businesses-need-to-know-commentary.html (Aufruf im Dezember 2017).

[4] Warner Bros. Pictures (Aufruf im Dezember 2017).

[5] BBC One (Aufruf im Dezember 2017).

[6] „Target Hackers Broke in Via HVAC Company“; Krebs on Security. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company (Aufruf im Dezember 2017).

[7] „#DefCon: Thermostat Control Hacked to Host Ransomware“; Infosecurity Magazine. https://www.infosecurity-magazine.com/news/defcon-thermostat-control-hacked (Aufruf im Dezember 2017).

[8] „Vom MSP zum MSSP“; SolarWinds MSP. http://pages.solarwindsmsp.com/path-to-mssp-wp-ungated.html (Aufruf im Dezember 2017).

GESCHÄFTSWACHSTUM DATENSICHERHEIT INTELLIGENTE AUTOMATISIERUNG

SolarWinds MSP unterstützt IT-Dienstanbieter mit Technik für die Erbringung eines professionellen und rentablen Service. Lokal installiert und in der Cloud bieten unsere Lösungen mehrschichtige Sicherheit, kollektive Intelligenz sowie intelligente Automatisierung und schaffen datenbasierte Einblicke, dank derer Provider ihre Arbeit schneller und einfacher erledigen. SolarWinds MSP hilft IT-Anbietern, sich auf das Wesentliche zu konzentrieren: die Erfüllung ihrer SLAs und den Aufbau eines gewinnbringenden Geschäftsmodells.