N-ABLE

HEAD NERDS

Playbook für Security Sales

Schützen & Wachsen: Chancen in der Cybersicherheit optimal nutzen

Umgang mit Einwänden und Schlüssel zum Erfolg

Dieses Digitale Playbook für Security Sales gibt MSPs eine wertvolle Hilfestellung beim Aufbau eines erfolgreichen Cybersecurity-Geschäfts. Es bietet eine Übersicht über die wichtigsten traditionellen Programme, die von MSPs erfolgreich beworben und verkauft werden, sowie Beispiele für Preisgestaltung, Verkaufsskripte und Marketingmaterialien, die Sie individuell anpassen können.

HAFTUNGSAUSSCHLUSS

Einleitung

Die richtige Preisgestaltung ist für viele MSPs nach wie vor eine der größten unternehmerischen Herausforderungen. Als Head Nerd im Bereich Vertrieb und Marketing erhalte ich oft Fragen von MSPs wie:

- „Wir hätten Interesse daran, [Name des Sicherheitsprodukts] in unser Angebot an Sicherheitslösungen aufzunehmen, aber das Preismodell für den Endkunden ist uns noch nicht ganz geheuer und hält uns doch irgendwie davon ab, es auf den Markt zu bringen."
- „Haben Sie Material zu den Vermarktungspreisen/-strategien für [Name des Sicherheitsprodukts]?"
- „Mein Kunde interessiert sich für [Name des Sicherheitsprodukts], aber ich bin mir nicht sicher, was ich dafür verlangen soll."

Also haben wir diesen Leitfaden zusammengestellt, um MSPs Strategien an die Hand zu geben, wie sie am besten mit diesen Arten von Vertriebs- und Preisanfragen umgehen können.

Die in diesem Leitfaden enthaltenen Tipps können auf JEDE Art von Produkt oder Dienstleistung angewendet werden, die ein MSP potenziell verkaufen möchte.

Ich hoffe, dass Ihnen dieses Playbook weiterhilft! Happy Selling!

Stefanie Hammond

Head Nerd – Vertrieb und Marketing

n-able.com/de/team-member/stefanie-hammond

Umgang mit Einwänden und Antworten zu Ihren mehrschichtigen Security-Programmen

Während des Vertriebsprozesses für traditionelle Managed-Services-Kunden werden Sie wahrscheinlich auf Vorbehalte stoßen oder Bedenken vom Geschäftsinhaber/CEO hören. Um Sie darauf vorzubereiten, haben wir nachfolgend die häufigsten Einwände aufgelistet, auf die Sie stoßen könnten, und jeweils einige mögliche Antworten dazu.

Tipp: Versuchen Sie, die direkten Zitate Ihres potenziellen Kunden während des Gesprächs festzuhalten, damit Sie diese in Ihr Angebot aufnehmen können, das Sie Ihrem potenziellen Kunden in der Abschlussphase unterbreiten

Die 12 häufigsten Einwände

„Ich dachte, ich wäre bereits geschützt? Wollen Sie damit sagen, dass das nicht der Fall ist?“	„Ich dachte, Sie kümmern sich bereits darum?“	„Warum muss ich die Dienstleistung wechseln?“	„Das klingt aber wesentlich teurer als das, was ich vorher bezahlt habe.“
„Das scheint mir den Preis nicht wert zu sein.“	„Das kann ich woanders billiger bekommen.“ oder „Ein anderer MSP verlangt nur X USD.“	„Kann ich einige Dienste streichen, damit das Ganze besser in mein Budget passt?“	„Ist EDR noch nicht genug? Jetzt sagen Sie mir, dass ich noch ein Produkt kaufen soll?“
„Das wird uns nicht passieren – wir sind zu klein.“	„Das wird uns nicht passieren. Wer würde denn unsere Daten wollen?“	„Ich lasse es darauf ankommen und zahle das Lösegeld und reiche den Schaden über meine Versicherung ein.“	„Nein. Ich werde nicht wechseln/ für dieses neue Programm nicht bezahlen.“

EINWAND NR. 1 & 2:

„Ich dachte, ich wäre bereits geschützt? Wollen Sie damit sagen, dass das nicht der Fall ist?“

„Ich dachte, Sie kümmern sich bereits für mich darum?“

Antwortbeispiel

„Sie waren geschützt und ich habe mich für Sie darum gekümmert. Aber genau wie sich die Bedrohungslandschaft weiterentwickelt, entwickelt sich auch die Technologie weiter, die benötigt wird, um weiterhin einen angemessenen und umfassenden Schutz zu bieten. Deshalb müssen sich auch die Dienstleistungen, die ich meinen Kunden anbiete, weiterentwickeln, um den Cyberkriminellen, die es da draußen gibt, immer einen Schritt voraus zu sein.

Für die ist das nur ein Geschäft und sie verdienen damit viel Geld. Im Jahr 2023 betrug die durchschnittliche Lösegeldzahlung 1,54 Millionen US-Dollar – fast doppelt so viel wie im Jahr 2022 mit 812.000 US-Dollar*. Wenn man allerdings die zahlreichen anderen Kosten berücksichtigt, die über die Lösegeldzahlung hinaus anfallen, kann sich der Schaden auf das Siebenfache** der ursprünglichen Lösegeldforderung belaufen.

Damit Ihnen und Ihrem Unternehmen so etwas nicht passiert, mussten wir unsere Sicherheitspakete ändern und wir müssen jetzt strengere Maßnahmen durchsetzen – nicht nur bei uns als Ihrem MSP, sondern bei allen unseren Kunden.“

https://www.varonis.com/blog/ransomware-statistics
**https://www.netapp.com/blog/ransomware-cost/#:~:text=In%20fact%2C%20the%20average%20ransom,cost%20of%20a%20ransomware%20attack

EINWAND NR. 3:

„Warum muss ich die Dienstleistung wechseln, die ich von Ihnen bekomme?“

Antwortbeispiel

„Es hat sich in den letzten drei bis fünf Jahren wahnsinnig viel verändert.

Statistiken zeigen, dass 60 % der KMU sechs Monate nach einem Cyberangriff schließen müssen* und wir möchten nicht dazu beitragen, dass es so weit kommt.

Daher empfehlen wir unseren Kunden die bewährten Sicherheitsverfahren, die wir noch im letzten Jahr empfohlen haben, heute nicht mehr.

Und wir werden dieses Gespräch höchstwahrscheinlich im nächsten Jahr wieder führen – bis dahin muss ich möglicherweise wieder neue Sicherheitsdienste einführen oder Änderungen vornehmen, weil Ransomware-Angriffe, Angriffe auf geschäftliche E-Mails und Phishing-Taktiken immer ausgefeilter werden.

Angesichts dieser sich ständig verändernden Bedrohungslandschaft muss ich als Ihr MSP auf dem Laufenden bleiben und meine Empfehlungen ständig anpassen, um die Netzwerke, Mitarbeiter und Daten unserer Kunden so sicher wie möglich zu halten.“

*https://purplesec.us/security-insights/top-cyber-attacks-2022/#Breaches

Fortsetzung …

Die Abbildung des mehrschichtigen Netzwerks kann verwendet werden, um Kunden zu erklären, WARUM sich die jetzt empfohlenen Sicherheitsdienste von den zuvor empfohlenen unterscheiden. Diese neuen Empfehlungen wirken sich dann in der Folge auf die Sicherheitspakete aus, die jetzt auf dem Markt beworben werden.

Betrachtet man die Customer Journey unter dem Gesichtspunkt der Sicherheit, so lautete die traditionelle Antwort der MSPs vor 5 bis 10 Jahren auf die Frage nach der Sicherheit: AV, Patchen, Firewall und Backup. Damals waren diese Dienste ausreichend, weil die Bedrohungen nicht so ausgeklügelt waren und die Leute in Büros hinter Firmen-Firewalls arbeiteten. In der heutigen Bedrohungslandschaft genügt das aber nicht mehr.

Wenn wir die grafische Darstellung eines mehrschichtigen Netzwerks mit dem klassischen Ansatz von AV/Patch/Firewall/Backup betrachten, fällt auf, dass manche Schichten nur unzureichend geschützt sind, während andere – insbesondere auf den Ebenen Cloud, Internet und Mensch – völlig ungeschützt sind. Dies hat zu erheblichen Sicherheitslücken bei Kunden geführt, wodurch der alte Mindeststandard für Basis-Sicherheit nicht mehr ausreicht. MSPs müssen daher ein umfassenderes Paket an Sicherheitsdiensten entwickeln und anbieten, um diese neu entstandenen Lücken zu schließen. Und der Fokus muss auch über den Endpunkt hinausgehen.

Neue Empfehlungen:

- **Änderungen auf Geräteebene:** Herkömmliche AV-Lösungen werden auf Geräteebene durch eine AV-Lösung der nächsten Generation wie **EDR** ersetzt, um einen umfassenderen, fortschrittlicheren Schutz vor Zero-Day-Bedrohungen zu bieten. Außerdem sind Rollback-Funktionen enthalten, mit denen das Gerät in einen funktionsfähigen Zustand vor dem Angriff zurückversetzt werden kann, falls doch etwas durchkommt

- **Internet-Ebene – Hinzufügen von**:
  - E-Mail-Sicherheit mit E-Mail-Filter und Spam-Schutz
  - Web-Sicherheit/DNS/URL-Filterung und
  - Darknet Monitoring

- **Netzwerk-Ebene – Hinzufügen von:** Netzwerkgeräteerkennung (mit einem Produkt wie **Ranger von SentinelOne**), das eine Warnung ausgibt, wenn neue, unbekannte Geräte wie IoT-Geräte oder Kamerasysteme im Netzwerk auftauchen, die versuchen könnten, Zugriff auf das Netzwerk zu erlangen

- **Mensch-Ebene – Hinzufügen von:**
  - Passwortmanagement
  - MFA (Multi-Faktor-Authentifizierung)
  - Sicherheitsschulungen für Benutzer

Fortsetzung …

- **Anwendungsebene – Hinzufügen von**:
  - Schwachstellenmanagement
  - Backup-Wiederherstellungstests mit der Möglichkeit, ein Standby-System zu implementieren
- **Cloud-Ebene – Hinzufügen von:** Managed Detection and Response, um die Sichtbarkeit, Überwachungs- und Erkennungsfunktionen zu verbessern und die Überwachung und Erfassung über den Endpunkt hinaus zu erweitern

Ein Ansatz mit mehrschichtigen Sicherheitsmaßnahmen bietet den besten Schutz vor Cyberangriffen, da jede Sicherheitslösung für sich genommen ihre eigenen Einschränkungen hat. Das Ziel ist es, so viele Hürden wie möglich zu errichten, um es Angreifern so schwer wie möglich zu machen, durchzukommen und einen Fuß in die Tür zu bekommen. Dann wird MDR implementiert, um die „Alarmglocken" zu läuten, wenn ein ungewöhnliches Verhalten festgestellt wird. Deshalb wird dringend davon abgeraten, Sicherheitsprodukte isoliert zu verkaufen und zu implementieren, da kein Produkt allein einen hundertprozentigen Schutz vor einem Angriff bieten kann.

Das mehrschichtige Netzwerk: Alte Sicherheitsempfehlungen – es gibt Lücken – Schichten sind unzureichend geschützt UND teilweise ungeschützt

Heute empfohlenes Sicherheitsprogramm: zielt darauf ab, die Lücken zu schließen, um sicherzustellen, dass ALLE Schichten ausreichend geschützt sind

EINWAND NR. 4 & 5:

„Das klingt aber wesentlich teurer als das, was ich vorher bezahlt habe.“

„Das scheint mir den Preis nicht wert zu sein.“

Antwortbeispiel

- Präsentieren Sie Ihren Kunden den ROI, um ihnen die Gesamtkosten zu verdeutlichen, die entstehen können, wenn sie nicht auf Ihr neues Sicherheitspaket umsteigen. So zeigen Sie, dass es günstiger ist, vorzubeugen, als Lösegeld zu zahlen. Die Zahlung von Lösegeld macht nur 15 % der Gesamtkosten eines Ransomware-Angriffs aus*
- 66 % der Unternehmen erlitten nach einem Angriff erhebliche Umsatzeinbußen**
- 53 % der Unternehmen gaben an, dass ihre Marke nach einem Angriff Schaden genommen hat**

*https://www.bleepingcomputer.com/news/security/ransom-payment-is-roughly-15-percent-of-the-total-cost-of-ransomware-attacks/
**https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

Darstellung des ROI über die Übung zu den Ausfallzeitkosten (pro Tag)

Ausfallzeitkosten = Produktivitätsverlust der Mitarbeiter + Umsatzverlust + Kosten für die Wiederherstellung + Kosten für nicht greifbare Verluste

Eine Version des ROI-Ausfallzeitrechners finden Sie HIER

Schritt 1: Kosten der verlorenen Mitarbeiterproduktivität berechnen (USD)

ROI – Kosten von Ausfallzeiten – Sicherheitsaspekt Kosten für Mitarbeiterproduktivität	
Vom Ausfall betroffene Abteilungen	**ALLE**
Anzahl der Mitarbeiter im Unternehmen	40
Anzahl der Mitarbeiter in der betroffenen Abteilung	40
Durchschnittlicher Produktivitätsverlust in %	100 %
Durchschnittliche Personalkosten pro Stunde	50 USD
Gesamtzahl der Ausfallstunden	160
Kosten für Mitarbeiterproduktivität	**320.000,00 USD**

Fortsetzung …

Beispiel:

- Steuerberatungskanzlei mit 40 Mitarbeitern
- Durchschnittliche Gehaltskosten = 50 $/Stunde
- Situation: Ein Mitarbeiter klickt auf einen Link in einer Phishing-E-Mail, die er erhalten hat, was eine Kettenreaktion auslöst und dazu führt, dass alle Mitarbeiter ausgesperrt werden
- Annahme: Die Dauer des Ausfalls beträgt 30 Tage
- Die Gesamtzahl der Ausfallstunden beträgt: *8 Stunden pro Tag *5 Tage pro Woche *4 Wochen = 160 Stunden

Kosten durch den Produktivitätsverlust der Mitarbeiter = 320.000 $

Schritt 2: Entgangene Einnahmen berechnen (USD)

Kosten für entgangene Einnahmen	
Bruttojahresumsatz	1.000.000,00 USD
Anzahl der Werktage pro Jahr für das Unternehmen	240
Anzahl der täglichen Arbeitsstunden	8
Anteil des unwiderbringlichen Geschäftsentgangs in %	100 %
Täglicher Einnahmenentgang	4.166,67 USD
Stündlicher Einnahmenentgang	520,83 USD
Einnahmenentgang für die Dauer des Ausfalls	**83.333,33 USD**

- Bruttojahresumsatz des potenziellen Kunden = 1 Mio. $/Jahr
- Annahme: Anzahl der Arbeitstage pro Jahr = 240 Tage
- Annahme: Anzahl der Arbeitsstunden pro Tag = 8
- Annahme: % der verlorenen Einnahmen, die möglicherweise nicht aufgeholt werden können = 100 %

Entgangene Einnahmen für die Dauer des Ausfalls = 83.333 $

Fortsetzung …

Schritt 3: Kosten für die Schadensbehebung berechnen (USD)

Wiederherstellungskosten	
Gesamtzahl der Arbeitsstunden bis zur vollständigen Wiederherstellung	160 USD
Stundensatz für Wiederherstellungsdienste	150 USD
Gesamtkosten für die Systemwiederherstellung	24.000 USD
Gesamtkosten für Ausfallzeiten	**427.333,33 USD**
Gesamtkosten für Ausfallzeit/Stunde	**2.670,83 USD**

- Gesamtzahl der Ausfallstunden (siehe oben) = 160 Stunden
- Stundensatz für Zeit- & Materialabrechnung = 150 $/Std.

Gesamtkosten für die Systemwiederherstellung, d. h. Gesamtkosten für die Schadensbehebung = 24.000 $

Gesamtkosten der Ausfallzeit = Kosten der verlorenen Mitarbeiterproduktivität + entgangene Einnahmen + Behebungskosten = 427.333 $

Kosten pro Stunde Ausfallzeit = 2.670 $/Stunde

Fortsetzung …

Schritt 4: Sonstige unbestimmte Kosten für nicht greifbare Verluste berechnen

Sonstige anfallende Kosten (Im Falle einer Sicherheitsverletzung)	
Kosten des Ransomware-Projekts	1.540.000,00 USD
Externe Forensik	
Bußgelder und Strafen (HIPAA, PCI)	
Kosten für Krisenkommunikation/Benachrichtigung	
Anwalts- & Rechtskosten	
Höhere Versicherungsprämien	
Beratungskosten + Gebühren für Mitarbeitersicherheitsschulungen	
Verbesserung der Infrastruktur	
Kollateralschäden	
Potenzielles Risiko für erneute Angriffe	
Verlust von Umsatz/Kunden	
Schädigung von Ruf, Marke & Geschäft	
Gesamtkosten der Sicherheitsverletzung	**1.967.333,33 USD**

KOSTEN EINES VERSTOSSES

- Die Kosten für die Ransomware-Zahlung bilden nur eine der Kostengruppen, die bei einer Sicherheitsverletzung anfallen
- Durchschnittliche Lösegeldzahlung im Jahr 2023 = 1.540.000 $* https://www.varonis.com/blog/ransomware-statistics
- Weitere potenzielle Kosten, die bei einer Sicherheitsverletzung entstehen können:
  - **Bußgelder** – Je nach Branche können Ihrem Kunden Bußgelder auferlegt werden, weil er keine angemessenen Vorsichtsmaßnahmen getroffen oder nicht in die erforderlichen Maßnahmen zum Schutz der personenbezogenen Daten seiner Kunden investiert hat.
  - **Kosten der Krisenkommunikation für Kunden** – Kunden, deren Daten möglicherweise kompromittiert wurden, müssen schriftlich benachrichtigt werden, damit sie vor betrügerischen Abbuchungen gewarnt sind. Das sind also zusätzliche Kosten, die für den Druck und den Versand von Briefen an Kunden sowie für die Personalkosten für die anschließende Bearbeitung von Kundenbeschwerden anfallen.

Fortsetzung …

- **Bußgelder** – Je nach Branche können Ihrem Kunden Bußgelder auferlegt werden, weil er keine angemessenen Vorsichtsmaßnahmen getroffen oder nicht in die erforderlichen Maßnahmen zum Schutz der personenbezogenen Daten seiner Kunden investiert hat.
- **Honorare für Rechtsanwälte und andere Rechtskosten,** die durch Sammelklagen und Einigungen entstehen, die von geschädigten Kunden eingereicht bzw. erzielt werden, nachdem sie erfahren haben, dass ihre Daten gestohlen und kompromittiert wurden. Solche Klagen können Unternehmen Summen im siebenstelligen Bereich kosten.
- **Höhere Versicherungsprämien** und höhere Selbstbehalte, die nach einem Cyberangriff eventuell von der Versicherungsgesellschaft erhoben werden.
- **Beraterkosten und Gebühren für Sicherheitsschulungen für Mitarbeiter** werden wahrscheinlich anfallen, um den Mitarbeitern beizubringen, worauf sie künftig achten müssen, damit es nicht zu einem weiteren Verstoß kommt.
- **Verbesserungen der Infrastruktur, Upgrades, neue Sicherheitstechnologien,** um Schwachstellen in der Sicherheitsinfrastruktur der Organisation zu beheben und den bestehenden Cybersicherheitsschutz zu stärken.
- **Kollateralschäden** – Die Sicherheitsverletzung könnte sich möglicherweise auf andere Organisationen in der Lieferkette des Kunden auswirken und deren Lieferanten und Kunden dauerhaft schädigen.
- **Risiko eines erneuten Angriffs** – die Gefahr, noch einmal Opfer eines Angriffs zu werden und dieselben Kosten erneut zu tragen!
- **Reputationsschaden für Marke und Unternehmen**, was in der Folge zu Umsatz- und Kundenverlusten führen kann.

Schritt 5: Gesamtkosten der Sicherheitsverletzung

Gesamtkosten der Sicherheitsverletzung = Gesamtkosten der Ausfallzeit + potenzielle Lösegeldzahlung + unbestimmte Kosten für nicht greifbare Verluste

Laut einer IBM-Studie könnten sich die unbestimmten Kosten für nicht greifbare Verluste auf bis zu 4,62 Millionen US-Dollar* belaufen (exklusive Lösegeldzahlung)

* https://www.netapp.com/blog/ransomware-cost/#:~:text=In%20fact%2C%20the%20average%20ransom,cost%20of%20a%20ransomware%20attack

Gesamtkosten der Sicherheitsverletzung = 427.333 $ + 1.540.000 $ + 4.620.000 $

Gesamtkosten der Sicherheitsverletzung = 6.587.333 $

Fortsetzung …

Schritt 6: ROI berechnen

ROI:	
Anzahl der Mitarbeiter	40 USD
Monatlicher Preis für das Managed Services-Programm	250 USD
Monatliche Kosten für das Security-Programm	**10.000 USD**
Jährliche Kosten für das Managed Services-Programm	**120.000 USD**
Ersparnis pro Jahr	**1.847.333,33 USD**

- Betrachtet man es aus der Perspektive des ROI:
- Monatliche Kosten für das Advanced Security Program = 250 $/Monat
- Organisation mit 40 Benutzern
- Monatliche Kosten für das Advanced Security Program = 10.000 $/Monat

Jährliche Kosten für das Advanced Security Program = 120.000 $/Jahr

Antwort zum Thema ROI:

„Wenn man die Kosten unseres Advanced Security Program – mit einer Jahresgebühr von 120.000 USD für den angemessenen Schutz Ihrer 40 Mitarbeiter – mit den Kosten vergleicht, die mit einer potenziellen Sicherheitsverletzung einhergehen, die ohne Weiteres 6 Millionen USD oder mehr übersteigen und auch das Risiko beinhalten können, dass Sie Ihre gesamte Existenzgrundlage und die Ihrer Mitarbeiter verlieren, lohnt es sich, auf Präventionsstrategien und Risikominderung zu setzen, statt zu einer Zahlung gezwungen zu werden.“

EINWAND NR. 6:

„Das kann ich woanders billiger bekommen.“ ODER „Ein anderer MSP verlangt nur X USD/Monat.“

- Möglichkeit: Das Programm des Konkurrenten enthält bestimmte wichtige Funktionen und Dienstleistungen nicht – dieser Mangel könnte der Grund für die Preisdifferenz sein
- Erinnern Sie den Kunden an die Illustrationen zur mehrschichtigen Sicherheit: Es gibt sechs wichtige Ebenen, die berücksichtigt werden müssen, wenn es darum geht, die kritischen Daten einer Organisation angemessen zu schützen, und alle sechs Ebenen erfordern ihre eigenen spezifischen Sicherheitstools

1. Perimeter-/Internet-Ebene
2. Netzwerk-Ebene
3. Benutzer-Ebene
4. Anwendungsebene
5. Geräte-Ebene
6. Cloud-Ebene

- Wenn ein Konkurrent behauptet, ein Cybersicherheitsprogramm für weit weniger als den von Ihnen verlangten Preis liefern zu können, sollten Sie sich fragen, was tatsächlich auf allen sechs Ebenen getan wird.
- Oder der Konkurrent unterschätzt den Arbeitsaufwand, der mit der erfolgreichen Umsetzung seiner Version des Programms verbunden ist, erheblich.
- Oder der Konkurrent opfert seine Gewinnspanne und seine Gesamtrentabilität, um den Auftrag zu erhalten, was auf lange Sicht keine nachhaltige Strategie ist, um ein erfolgreiches Unternehmen aufzubauen.
- Zur Erinnerung: Die besten MSPs ihrer Klasse erwirtschaften mit ihren Cybersicherheitsprogrammen eine Bruttomarge zwischen 60 und 80 % oder mehr. Diese Programme sollten also mehr kosten, da MSPs für die von ihnen angebotenen Sicherheitsprogramme einen angemessenen Preisaufschlag verlangen sollten.
- Um diesen Einwand zu entkräften, nutzen Sie den niedrigeren Preis des Konkurrenten als Argument und ergreifen Sie die Gelegenheit, um nicht nur Ihre umfassenden Sicherheitstools hervorzuheben, sondern auch die Qualifikationen Ihrer hochqualifizierten Mitarbeiter sowie die bewährten Verfahren und Prozesse, die Sie dank der Einhaltung diverser Compliance- und Sicherheitsvorschriften implementieren.

Antwortbeispiel:

„Unsere monatliche Gebühr entspricht dem, was wirklich benötigt wird, um unsere Kunden angemessen vor Cyber-Problemen zu schützen, diese zu erkennen, zu beheben und sich davon zu erholen. Eine vernünftige Risikominderung ist eine Kombination aus der Implementierung der richtigen Tools und der richtigen Abläufe und Verfahren. Ich befürchte, dass der Preis, der Ihnen genannt wurde, nicht alles enthält, was heute von Compliance-Standards und Anbietern von Cyber-Haftpflichtversicherungen empfohlen wird.“

EINWAND NR. 7:

„Kann ich einige der Leistungen, die Sie in das Programm aufgenommen haben, streichen, die ich meiner Meinung nach nicht wirklich brauche, damit die monatliche Gebühr besser in unser Budget passt?“

- Kurz gesagt: Nein – es wird dringend empfohlen, dass Sie Kunden nicht die Möglichkeit geben, aus Kostengründen Leistungen zu streichen.
- Es ist nicht ratsam, Kunden zu gestatten, ihren eigenen Support-Weg zu diktieren.
- Erinnern Sie sich an die Grafik mit den sechs Sicherheitsebenen, die die Mitarbeiter und kritischen Daten Ihres Kunden umgeben. Wenn ein MSP seinen Kunden erlaubt, Dienste aus Budgetgründen wegzulassen, entstehen Lücken im Schutz des Kunden, wodurch das Risiko steigt, dass Malware oder ein Virus eindringt.
- Die Programme wurden so konzipiert, dass jede der sechs Ebenen angemessenen Schutz erhält, um die bestmögliche Verteidigung aufzubauen, und auch eine schnellere Wiederherstellung zu ermöglichen, wenn etwas passiert (denn die Frage ist nicht, OB etwas passiert, sondern WANN).
- Ziel des traditionellen Sicherheitsprogramms ist es, die Mitarbeiter mit möglichst geringen Schäden und möglichst geringen Auswirkungen wieder an die Arbeit zu bringen.
- Wenn der Preis oder das Budget ein Problem darstellen, insbesondere wenn dieser Einwand von einem bestehenden Break/Fix- oder A-la-carte-/Reaktivkunden geäußert wird, positionieren Sie das Essential Security Program als das minimal realisierbare Sicherheitsprogramm, in das Kunden integriert werden können.
- Wenn der MSP die Streichung von Leistungen zulässt, um ein bestimmtes Preisniveau zu erreichen, erhöht sich das Risiko und die Gefahr der Haftung für ihn selbst und seine Kunden.
- Es entstehen nicht nur Kosten für den Kunden, wenn er sich weigert, seine Sicherheitsvorkehrungen zu erhöhen (erinnern Sie sich an die ROI-Übung, die wir zuvor besprochen haben), auch dem MSP könnten finanzielle Kosten entstehen, wenn ein Mindestsicherheitsstandard nicht durchgesetzt wird, wie z. B.:
  - **Umsatzverlust** – Bei einer durchschnittlichen Behebungszeit von 30 Tagen und Kosten von etwa 24.000 USD oder mehr (aus unserem vorherigen Beispiel für ROI/Kosten von Ausfallzeiten) handelt es sich um erhebliche, unerwartete Kosten für ein kleines Unternehmen. Oftmals gewähren MSPs einen hohen Rabatt auf diese Rechnung oder erlassen sie ganz, weil sie sich schuldig fühlen, dass ein Angriff durchgekommen ist.
  - **Imageschaden** – Genau wie bei einem Kunden, der Opfer einer Datenschutzverletzung wird und je nach Verlauf einen Imageschaden erleiden kann, könnte auch der MSP einen Imageschaden erleiden, wenn bekannt wird, dass trotz seiner Dienste eine Datenschutzverletzung stattgefunden hat. Dies könnte besonders nachteilig sein, wenn dieser MSP branchenspezifisch tätig ist.

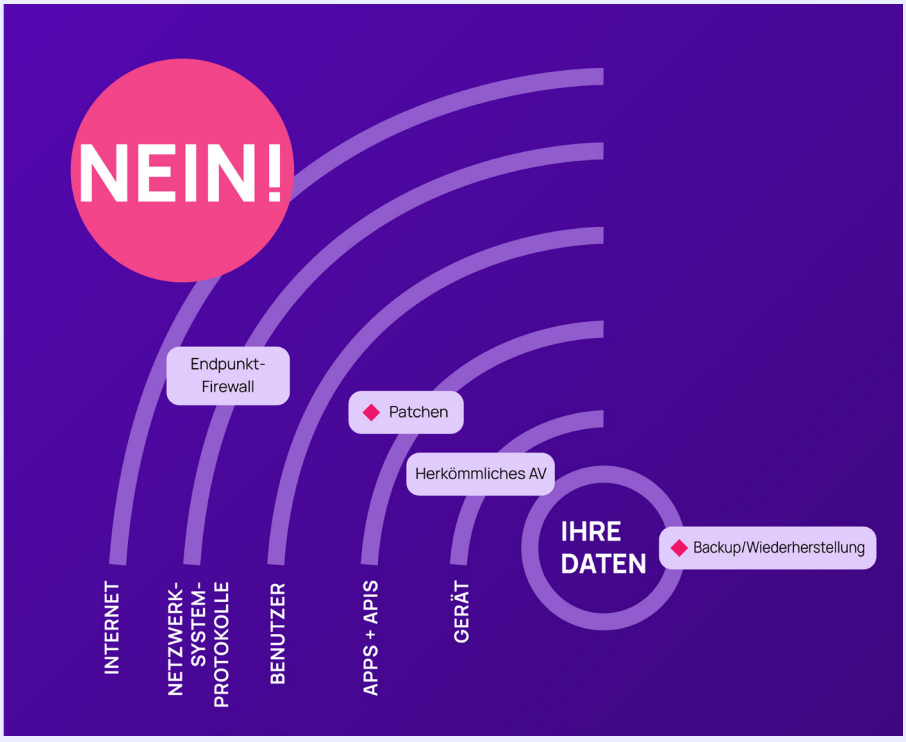
Fortsetzung …

- **Schadensersatzkosten/Bußgelder** – Der MSP könnte mit einer Geldstrafe belegt oder verklagt und für fahrlässig befunden werden, was für ihn das Aus bedeuten könnte.
- **Opportunitätskosten und entgangene Umsätze** aufgrund des Verlusts anderer potenzieller Geschäfte, die der MSP in dieser Zeit hätte abschließen können, die aber nicht zum Abschluss kamen, weil seine erfahrensten Techniker abgestellt werden mussten, um dem Kunden bei der Behebung des Sicherheitsverstoßes zu helfen.
- **Betriebskosten** – Wenn Kunden die Möglichkeit eingeräumt wird, Leistungen aus dem Mindestpaket zu entfernen, wird es schwieriger, Kunden im Alltag zu verfolgen, abzurechnen, zu unterstützen und zu betreuen, da jeder Kunde ein wenig anders wäre. Dies führt dazu, dass der MSP viele Vorteile in Bezug auf Serviceoptimierung und Effizienz einbüßt, die durch die Programmstandardisierung erzielt werden können.

Antwortbeispiel:

„60 % der kleinen und mittleren Unternehmen gehen innerhalb von 6 Monaten nach einem Cyberangriff pleite*, dieses Schicksal möchten wir unseren Kunden ersparen. Wir haben unsere Sicherheitsprogramme so konzipiert, dass jede Ebene zwischen Ihren Mitarbeitern, den Daten, auf die sie zugreifen, und der Außenwelt angemessen geschützt ist. Und wenn wir eine Dienstleistung herausnehmen, reißen wir ein Loch in diesen Schutz und erhöhen damit die Wahrscheinlichkeit, dass sie Opfer eines Angriffs werden.“

*https://purplesec.us/security-insights/top-cyber-attacks-2022/#Breaches



EINWAND NR. 8:

„Was ist denn mit dieser Endpoint Detection and Response Lösung, von der Sie mir letztes Mal erzählt haben? Reicht das nicht? Sie haben mir damals gesagt, dass ich das brauche, und jetzt sagen Sie mir, dass ich noch mehr Produkte kaufen muss? Das sieht mir nach reiner Geldmacherei aus.“

Dieser Einwand gilt für alle MSPs, die möglicherweise immer noch Sicherheit auf Einzelproduktbasis verkaufen, anstatt eine komplette Sicherheitslösung im Paket anzubieten. Die folgende Antwort kann dem MSP aus dieser Situation helfen.

Antwortbeispiel

„Endpoint Detection and Response (EDR) ist nach wie vor notwendig, sie ist aber nur ein Teil der gesamten Sicherheitslösung, die wir unseren Kunden jetzt empfehlen. Als Ihr MSP muss ich Ihre Organisation rund um die Uhr an 365 Tagen im Jahr schützen und sicherstellen, dass Ihr Unternehmen keine unnötigen, langen Ausfallzeiten erleidet, die sich auf Ihren Umsatz und Ihren Ruf auswirken könnten. Unser Ziel ist es, Ihr Unternehmen funktionsfähig und betriebssicher zu halten – und dafür müssen wir unseren Schutz über den Endpunkt hinaus erweitern.

Leider sehen wir mit nur einem Tool zum Schutz und zur Erkennung am Endpunkt nicht alles, was im gesamten Netzwerk passiert. Der Endpunktschutz sieht nur, was am Endpunkt geschieht, und der Endpunkt ist nicht immer der Einstiegspunkt für einen Angreifer. Bei einem Angriff kann er uns nicht das vollständige Bild davon vermitteln, wie dieser Angriff begonnen hat oder was passiert ist, und das brauchen wir aus forensischer Sicht, insbesondere wenn wir einen Schadensfall einreichen und Ihre Cyber-Haftpflichtversicherung einschalten müssen.

Wenn wir also andere Technologiekomponenten zum Schutz der Ebenen jenseits des Endpunkts einbeziehen und dann unseren ganzheitlicheren Managed Detection and Response Service darüber hinaus integrieren, bietet dies eine umfassendere Abdeckung und ein höheres Maß an Transparenz, was uns helfen wird, wenn wir Ihnen bei der Wiederherstellung nach einem Cyberangriff oder einem Datenschutzverstoß helfen müssen. Ein EDR-Agent allein am Endpunkt reicht nicht mehr aus, um uns die Sichtbarkeit und den Umfang an Abdeckung und Daten zu bieten, die wir heute benötigen.

Das Fazit lautet also: Wir verkaufen kein Produkt mehr als Einzellösung, weil wir wissen, dass es keine 100-prozentige Sicherheit vor Angriffen gibt. In Zukunft werden wir verschiedene Dienste und Sicherheitstools zu einem Advanced Security Program zusammenfassen, da dies die beste Verteidigung ist, um das Cyberrisiko für unsere Kunden zu minimieren und die Wahrscheinlichkeit zu verringern, dass sie einem Angriff zum Opfer fallen.“

EINWAND NR. 9 & 10:

„Das wird uns nicht passieren. Wir sind zu klein und wurden noch nie angegriffen."

ODER

„Das wird uns nicht passieren. Wer würde denn unsere Daten wollen?"

- „Sicherheit durch Unbekanntheit ist keine Sicherheitsstrategie für kleinere Unternehmen." Charles Weaver – MSP Alliance
- Dass ein Kunde hofft, aufgrund seiner Größe oder der Tatsache, dass er noch nie Opfer eines Angriffs geworden ist, nicht ins Visier von Angreifern zu geraten, ist keine Schutzstrategie, die Sie als MSP akzeptieren sollten.
- Die Größe des Kunden spielt keine Rolle mehr – nach Angaben des CISA sind kleinere Unternehmen dreimal so gefährdet, angegriffen zu werden, wie größere. (https://www.cisa.gov/news-events/news/accelerating-our-economy-through-better-security-helping-americas-small-businesses-address-cyber)
- Jedes Unternehmen kann angegriffen werden.
- Es könnte sein, dass das Unternehmen nicht das eigentliche Ziel ist, aber Cyberkriminelle könnten auf der Suche nach Zugang zu den Lieferanten und Anbietern sein, mit denen der Kunde geschäftliche Beziehungen unterhält, und daher könnte der Kunde als potenzielles Einfallstor zu diesen anderen, begehrteren Anbietern dienen.
- Daher ist Aufklärung gefragt, um dem Kunden zu verdeutlichen, dass er zwar „glaubt", dass ihm kein Angriff passieren könnte, dass der aktuelle Zustand seines Netzwerks jedoch nicht den neuen Sicherheitsstandards entspricht, die Ihr MSP für alle Kunden festgelegt hat. Deshalb muss die Netzwerksicherheit verstärkt werden, um zu vermeiden, dass das Netzwerk zum „schwächsten Glied" in der Kette zu seinen Lieferanten und Geschäftspartnern wird, mit denen er interagiert.
- Auch wenn der Kunde abwinkt und sagt, dass er sich nicht für eines Ihrer mehrschichtigen Sicherheitsprogramme anmelden muss, weil niemand seine Daten haben will, ist wiederum Aufklärung gefragt.
- Die Angreifer interessieren sich nicht zwangsläufig für die Daten, die sie stehlen, sie sind nur an dem Lösegeld interessiert, das sie kassieren könnten. Sie wissen natürlich ganz genau, dass dem Kunden seine Daten sehr wohl wichtig sind, und daraus schlagen sie Profit.
- Bei kleineren Kunden haben die Bösewichte leichtes Spiel und können schnell punkten, nicht zuletzt aufgrund der Art und Weise, wie sie in der Vergangenheit von MSPs behandelt wurden.

Antwortbeispiel

„Cyberangriffe auf kleine Unternehmen haben in den letzten Jahren sogar zugenommen, weil sie wegen ihrer nachlässigen Sicherheitsvorkehrungen leichte Beute sind. Tatsächlich richten sich bestimmte Arten von Angriffen – Social-Engineering-Angriffe wie Phishing – viel häufiger gegen kleinere Unternehmen.*

Schon gewusst? 61 % der KMU waren 2021 Ziel eines Cyberangriffs und 37 % der Ransomware-Angriffe richteten sich gegen KMU mit weniger als 100 Mitarbeitern.*

Fortsetzung …

Das Traurige daran ist, dass kleinere Unternehmen in der Regel finanziell nicht auf einen Angriff vorbereitet sind und viele keine angemessene Cyberversicherung haben. Ein erfolgreicher Angriff auf ein kleineres Unternehmen könnte es daher möglicherweise in den Ruin treiben, und genau das wollen wir mit unseren Sicherheitsprogrammen für unsere Kunden verhindern."

*https://www.strongdm.com/blog/small-business-cyber-security-statistics (aufgerufen im März 2024)

EINWAND NR. 11:

„Ich lasse es darauf ankommen und zahle das Lösegeld und reiche den Schaden über meine Versicherungsgesellschaft ein."

- Wenn Sie eine solche Antwort von einem Kunden erhalten, sollten Sie ernsthaft darüber nachdenken, ob Sie diese Geschäftsbeziehung fortsetzen möchten. Dies ist ein Warnsignal – Sie können nicht zulassen, dass sich ein Kunde ausschließlich auf seine Versicherungsgesellschaft verlässt, um ihm aus der Patsche zu helfen.
- Die Cyber-Versicherungsbranche befindet sich aufgrund der gestiegenen Anzahl von Angriffen und der höheren Auszahlungen, zu denen sie zunehmend gezwungen war, im Wandel. Daher beginnt sie, die Spielregeln zu ändern.
- Wenn eine Organisation Lösegeld zahlen muss und einen Antrag auf Kostenübernahme stellen möchte, wird die Versicherungsgesellschaft wahrscheinlich zunächst eine Untersuchung durchführen wollen, was Zeit in Anspruch nimmt.
- Erinnern Sie den Kunden daran und weisen Sie ihn darauf hin, dass Ausfallzeiten sein Unternehmen Geld in Form von entgangenen Einnahmen und Produktivitätsverlusten kosten werden.
- Und wenn die Versicherungsgesellschaft ihre Untersuchung durchführt, besteht ihr Ziel darin, die fahrlässige Partei zu ermitteln und festzustellen, wer möglicherweise schuldhaft gehandelt hat.
- Ihr Ziel – als MSP dieses Kunden – ist es, nicht als die fahrlässige Partei eingestuft zu werden, und Sie möchten auch nicht, dass Ihr Kunde als fahrlässig eingestuft wird, was dazu führen könnte, dass eine Kostenübernahme abgelehnt wird.
- Und wenn nicht die richtigen Sicherheitsmaßnahmen ergriffen werden, könnte die Versicherungsgesellschaft das zum Anlass nehmen, die Versicherung des Kunden für nichtig zu erklären und die Zahlung abzulehnen.
- Sowohl der MSP ALS AUCH der Kunde müssen bestimmte Anforderungen erfüllen, die von den Cyber-Haftpflichtversicherungen festgelegt wurden, um die Chancen auf eine Auszahlung im Schadensfall zu erhöhen:
  - MSPs müssen nachweisen, dass sie mit allen ihren Kunden Gespräche über Cybersicherheit und Risiken führen, um ihre eigenen Cyber-Versicherungspolicen verlängern zu können.

Fortsetzung …

- Wenn der MSP mit seinen Kunden nicht über die Haftung und das Risiko im Bereich der Cybersicherheit redet oder wenn er sie nicht dazu verpflichtet, sich für eines seiner neuen Sicherheitsprogramme anzumelden, oder wenn er seinen Kunden erlaubt, sein Sicherheitsprogramm abzulehnen, ohne dass sie eine Freistellung oder einen Haftungsausschluss unterschreiben, dann wird die Versicherungsgesellschaft den MSP als fahrlässige Partei identifizieren und es besteht eine hohe Wahrscheinlichkeit, dass eine Kostenübernahme abgelehnt wird, da der MSP nicht nachweisen kann, dass er seiner Sorgfaltspflicht nachgekommen ist und die richtigen Schritte zum Schutz seines Kunden unternommen hat.
- Der Kunden muss wiederum nachweisen, dass er die richtigen Schutzmaßnahmen ergriffen hat, um sein Netzwerk angemessen zu verwalten und zu schützen.
- Und wenn nachgewiesen wird, dass der MSP angeboten hat, ihn in eines seiner Cybersicherheitspakete (das den Anforderungen des Antrags auf eine Cyberhaftpflichtversicherung entspricht) aufzunehmen, der Kunde diesen Schutz jedoch abgelehnt hat, dann hat die Versicherungsgesellschaft ebenfalls ihre fahrlässige Partei gefunden und kann sich möglicherweise weigern, für den Schaden aufzukommen.

- Indem der MSP die Aufnahme in eines der strukturierten Sicherheitsprogramme vorschreibt, haben sowohl der MSP als auch der Kunde gezeigt, dass sie die richtigen Schritte unternommen haben, um sich vor einem Cyberangriff zu schützen, und damit die Wahrscheinlichkeit erhöht, dass die Versicherungsgesellschaft im Schadensfall zahlt.

EINWAND NR. 12:

„Nein. Ich werde weder zu Ihrem neuen Programm wechseln noch für diese neuen Dienstleistungen bezahlen.“

Antwortbeispiel Nr. 1

Wenn es sich bei diesem Kunden um einen Mandanten aus dem Rechts- oder Gesundheitswesen handelt, der diesen Widerstand leistet, könnte eine mögliche Reaktion lauten:

- „Herr Kunde/Frau Kundin, ihre Aufgabe ist es, Ihre Kunden zu schützen. Und das ist auch meine Aufgabe. Aber indem Sie sich weigern, sich für mein neues Sicherheitsprogramm anzumelden, das ich entwickelt habe, um meine Kunden besser zu schützen, hindern Sie mich daran, meine Arbeit zu tun. Und ich habe das Gefühl, dass Sie meinen Job als Ihr Berater für IT-Sicherheit nicht ernst nehmen, wenn ich Ihnen Empfehlungen gebe, um Ihre Mitarbeiter und Ihr Unternehmen zu schützen. Es ist notwendig, dass Sie diesen neuen Vertrag für unser neues Cybersicherheitsprogramm unterzeichnen, das wir ab jetzt standardisieren und in das wir alle unsere Kunden aufnehmen.“

Fortsetzung …

Wenn Sie weiterhin auf Widerstand stoßen und der Kunde den neuen Vertrag bei diesem Treffen nicht unterschreibt, fragen Sie anschließend nach:

- „Wenn Sie das Gefühl haben, dass Sie diese neue Vereinbarung jetzt gerade nicht unterzeichnen können, wie sieht es dann in Zukunft aus? Könnten Sie in den nächsten 60 bis 90 Tagen unterschreiben?“

Hoffentlich wird der Kunde seine Entscheidung überdenken, insbesondere wenn Sie ihm eine kurze Frist einräumen, um sich an den Gedanken an die von Ihnen vorgenommenen Änderungen zu gewöhnen.

Antwortbeispiel Nr. 2

Wenn der Kunde sich immer noch weigert, Ihren neuen Vertrag zu unterzeichnen und sich weigert, in eines Ihrer neuen Sicherheitsprogramme aufgenommen zu werden, dann legen Sie eine Strategie fest, um diese risikoreichsten Kunden in weniger riskante Kunden für Ihr Unternehmen umzuwandeln, denn Sie können schließlich nicht zulassen, dass sie zu einer Bedrohung für Ihren Lebensunterhalt oder den Ihrer Mitarbeiter werden.

Einige Optionen:

- Lassen Sie den Kunden eine neue Rahmenleistungsvereinbarung unterzeichnen, die einen Haftungsausschluss/eine Haftungsbeschränkung/eine Haftungsfreistellung enthält.
- Lassen Sie sie eine Risikoakzeptanzerklärung unterzeichnen, zusammen mit der Anerkennung des neuen Tarifplans und der SLO, in der ihre neuen Tarife und Reaktionszeiten für den Fall, dass sie Unterstützung anfordern müssen, dargelegt sind.
- In der Regel erhöhen MSPs ihre Zeit- und Materialkosten für Nicht-Standardkunden (als solche wird dieser Kunde nun definiert) auf das 2- oder 3-fache ihrer Standard-Zeit- und Materialkosten und führen neue, längere Reaktionszeiten ein, da Kunden in Standard-Sicherheitsprogrammen nun Vorrang erhalten.

Wenn der Kunde diese Art von Dokumenten unterschreibt, hat der MSP einen Nachweis, um der Versicherungsgesellschaft zu zeigen, dass er versucht hat, mit seinem Kunden ein Gespräch über Sicherheit, Risiko und Compliance zu führen, der Kunde jedoch den angebotenen Schutz abgelehnt hat.

Antwortbeispiel Nr. 3

Wenn der Kunde sich weiterhin weigert, den neuen Vertrag zu unterzeichnen, könnten Sie sich eventuell dazu entscheiden, die Geschäftsbeziehung zu beenden, da der Kunde nicht mehr zu Ihrem Unternehmen passt.

- „Ich respektiere Ihre Entscheidung, kann diese aber leider nicht unterstützen. Sie birgt ein erhebliches Risiko, dem wir uns nicht aussetzen können. Unsere Aufgabe ist es, unsere Kunden und ihr Unternehmen zu schützen. Wenn Sie sich nicht für unser empfohlenes Sicherheitsprogramm anmelden, beeinträchtigt dies unsere Fähigkeit, das zu tun, was gemäß den bewährten Verfahren für Sicherheit und Compliance erforderlich ist. In diesem Fall ist es für Sie möglicherweise besser, mit einem anderen MSP zusammenzuarbeiten, der sich nicht an die von uns empfohlenen Sicherheitsstandards hält. Wir helfen Ihnen gerne bei der Umstellung auf einen anderen MSP.“

Letztendlich liegt die Entscheidung beim Kunden – aber lassen Sie diese Angelegenheit nicht länger als 60 bis 90 Tage offen, da Sie damit Ihr MSP-Unternehmen gefährden.

Der Schlüssel zum Erfolg in Marketing und Vertrieb

Unabhängig davon, welche Art von Sicherheitsprogramm Sie entwickeln und auf den Markt bringen, hier noch ein paar abschließende Bemerkungen:

1 Achten Sie darauf, die richtige Art von Kunden auszuwählen, mit denen Sie Geschäfte machen möchten, und vergewissern Sie sich, dass diese gut zu Ihrem Geschäftsmodell passen.

Denken Sie in Ihrer Planungsphase über Ihr ideales Kundenprofil nach, definieren Sie die Arten von Unternehmen, die Sie für beide Kategorien von Kunden haben möchten, und kommunizieren Sie dieses Ideal an alle Mitglieder Ihres Teams.

2 Konzentrieren Sie sich auf Ihre Botschaft und darauf, wie Sie Ihre Wertversprechen formulieren.

Denken Sie bei der Erstellung Ihres GTM-Plans für Ihre Sicherheitsdienste wie ein CEO oder ein CFO und überlegen Sie, was solche Führungskräfte vorrangig interessiert.

Ihnen ist Folgendes wichtig:

- Rentabilität
- Wachstum
- Skalierbarkeit
- Minimierung jeglicher Risiken, die das Wachstum ihrer Organisation behindern oder hemmen können

Überlegen Sie auch, was dem IT-Führungsteam am wichtigsten ist!

Ihm ist Folgendes wichtig:

- Erfolgreicher und termingerechter Abschluss wichtiger IT-Projekte
- Kompetente und effiziente Erledigung der täglichen Aufgaben, die für die ordnungsgemäße Pflege ihrer Netzwerkinfrastruktur erforderlich sind

- Schaffung und Aufrechterhaltung einer zuverlässigen und stabilen Netzwerkumgebung, damit die Mitarbeiter produktiv arbeiten können
- Aufrechterhaltung der Mitarbeitermoral und Sicherstellung, dass ihre technischen Mitarbeiter engagiert und motiviert zur Arbeit kommen
- Reduzierung der Abwanderung von technischen Mitarbeitern durch die Schaffung einer positiven Work-Life-Balance
- Minimierung des Risikos für die Organisation und Schutz des Unternehmens und seiner kritischen Daten mit allen verfügbaren Mitteln

3 Kümmern Sie sich vor dem Start um die Marketinggrundlagen.

Stellen Sie sicher, dass die folgenden Maßnahmen abgeschlossen und umgesetzt sind:

- Ihre Webseite ist auf dem neuesten Stand und enthält die neuen Informationen zu Ihren Sicherheitsdiensten.
- Ihre Unternehmens- und persönlichen LinkedIn- und Google-Business-Profile wurden aktualisiert, um die neuen Dienstleistungen Ihres MSP-Unternehmen bekannt zu geben.
- Sie haben ausreichend Erfahrungsberichte von bestehenden Kunden gesammelt und/oder Fallstudien erstellt, um zu zeigen, wie Ihre Dienstleistungen zum Erfolg ihrer Unternehmen beigetragen haben.
- Sie haben eine proaktive Telemarketing-Aktion für den Vertrieb durchgeführt, bei der potenzielle Kunden angerufen wurden, um Interesse und Aufmerksamkeit zu wecken.

N-able bietet MSPs und IT-Serviceanbietern leistungsstarke Software zur Überwachung, Verwaltung und Absicherung von IT-Infrastrukturen und Netzwerken. Unser Angebot umfasst eine skalierbare Plattform, eine sichere Infrastruktur, Tools für die einfachere Verwaltung komplexer IT-Umgebungen und Ressourcen für die digitale Transformation. Wir unterstützen unsere Partner in jeder Wachstumsphase beim Schutz ihrer Kunden sowie beim Ausbau ihres Angebots – durch das ständig wachsende flexible Portfolio an Integrationen führender Anbieter. n-able.com/de

---