Marktüberblick:
Cyberbedrohungen heute

MSP-Sicherheit auf neuem Niveau

N-ABLE™

Eine unabhängige Umfrage im Auftrag von N-able

Die Welt ändert sich – Unternehmen müssen sich anpassen

Managed Services Provider (MSPs) sind in der Pandemie außergewöhnlich stark gefordert. Unter unsicheren und immer neuen wirtschaftlichen Bedingungen müssen sie nicht nur den reibungslosen Geschäftsbetrieb ihrer Kunden sicherstellen, sondern sich auch selbst auf die neue Lage einstellen, wenn sie wirtschaftlich überleben wollen.

Unter diesen schwierigen Umständen haben Cyberkriminelle offensichtlich schnell ihre Chance gewittert: Online-Angriffe haben nach dem Ausbruch der Pandemie beträchtlich zugenommen. Immer häufiger werden inzwischen auch MSPs zur Zielscheibe, da sie in Beziehung zu Unternehmen stehen, deren Systeme Kriminelle gerne kapern möchten, um sensible Daten zu erbeuten.

Eine neue Umfrage von N-able (in Zusammenarbeit mit Coleman Parkes Research) geht nun der Frage nach, welche Rolle MSPs spielen, auch im Hinblick auf die Sicherheit ihrer Kunden. Wie stark sind MSPs selbst bedroht? Welche Schutzmaßnahmen sollten sie kennen? Worauf sollten sie sich bei der Implementierung erforderlicher Lösungen konzentrieren, um sich selbst und ihre Kunden abzusichern? Die neue Umfrage gibt hierauf Antwort.

Tatsache ist: Unternehmen sind heutzutage keine isolierten Betriebe mehr, sondern über eine globale Infrastruktur und digitale Supply Chain miteinander verbunden. Das macht uns alle zum Angriffsziel. Also geht es uns alle etwas an.

ZUSAMMENFASSUNG DER UMFRAGEERGEBNISSE:[1]

- MSPs sind immer häufiger ein direktes Ziel von Cyberangriffen.
- Fast alle MSPs waren in den letzten 18 Monaten Opfer eines Cyberangriffs.
  90 % verzeichnen eine Zunahme der Angriffe seit dem Ausbruch der Corona-Pandemie.
- 82 % der Kunden von MSPs verzeichnen eine Zunahme der Angriffsversuche.
- MSPs vergrößern ihr Sicherheitsbudget im Durchschnitt um 5 %.
  Ob dies ausreicht, bleibt fraglich.
- Die Automatisierung wichtiger Elemente ist entscheidend, um Kriminellen einen Schritt voraus zu bleiben.
- Backup gehört zum Standardangebot der MSPs, doch nur 40 % sichern Workstations alle 48 Stunden oder häufiger. Hier besteht Verbesserungsbedarf.
- Nur 40 % der MSPs schützen die eigenen Systeme mit Zwei-Faktor-Authentifizierung (2FA).
  MSPs müssen die Basiselemente der Sicherheit noch stärker in den Fokus nehmen.
- KMU weiten derzeit ihre Sicherheitsbudgets aus. MSPs haben dadurch die Chance, mehr Umsatz und bessere Angebote zu machen.

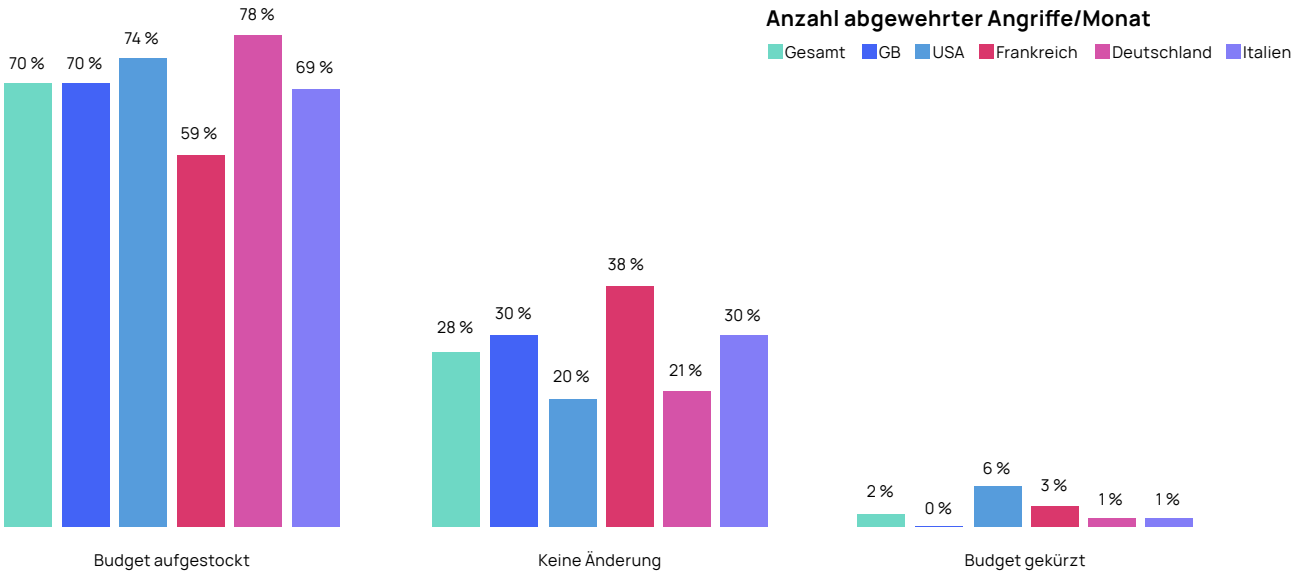
[1] Alle im Dokument genannten Zahlen basieren auf den Ergebnissen der unabhängigen Umfrage im Auftrag von N-able.

KMU erhöhen ihre Sicherheitsbudgets

Bevor sie ihre eigene Sicherheitsstrategie überdenken, sollten MSPs wissen, wofür genau ihre Kunden Geld auszugeben gedenken. Viele Unternehmen haben harte Jahre hinter sich. Mehr Sicherheit ist fraglos wichtig, doch vielleicht haben derzeit nicht alle KMU dafür ein offenes Ohr.

Allerdings lassen die Zahlen hoffen: Unserem Bericht zufolge haben 7 von 10 KMU vor, ihr Sicherheitsbudget aufzustocken. In Frankreich fällt der Wert etwas ab, doch auch dort sind es immerhin noch 6 von 10 KMU.

Der Anteil derer, die nicht aufstocken, behält größtenteils das bisherige Budget bei; nur 2 % erwägen Kürzungen. Die Budgeterweiterungen betragen im Durchschnitt 7 % und sind somit erheblich. Angesichts der aktuellen Umstände investieren die Unternehmen also solide in ihre Sicherheit.



Dieser Trend bedeutet für MSPs gute Umsatzchancen. Vielen Kunden leuchtet auf Anhieb ein, dass Sicherheit wichtig ist und sie hier investieren müssen. Entscheidend für MSPs ist eher die Frage, wo am besten investiert werden soll und wie sie aus den Mehrinvestitionen optimal Kapital schlagen.

KMU möchten ihr Budgetplus vorrangig in Datensicherheit und Cloud-Sicherheit investieren; Identität und Zugriff stehen auf der Prioritätenliste ganz hinten. Wenn es darum geht, ergänzende oder bessere Dienste anzubieten, sollten MSPs die Vorstellungen ihrer Kunden natürlich bis zu einem gewissen Grad bedienen, darüber aber nicht ihre Rolle als Experte aus dem Auge verlieren.

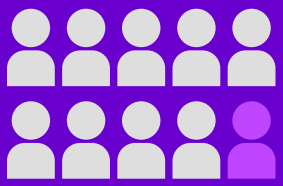
- Datensicherheit
- Cloud-Sicherheit
- Absicherung der Infrastruktur
- Sicherheitsdienste
- Netzwerksicherheit
- Anwendungssicherheit
- Risk Intelligence
- Identitäts- und Zugriffskontrolle

MSPs im Fadenkreuz von Cyberkriminellen

Cyberangriffe sind inzwischen ständig in den Schlagzeilen. Schwere Ransomware-Angriffe beeinträchtigen weltweit digitale Supply Chains oder schädigen Versorgungsinfrastrukturen.

MSPs sind als lohnendes Angriffsziel schon lange im Visier von Verbrechern, denn sie bieten guten Zugang zur Supply Chain: Wer in das System eines MSPs eindringt, hat darüber auch sofort Zugriff auf die Daten und Systeme seiner Kunden. In der Corona-Pandemie haben Kriminelle die MSP-Sparte noch schärfer ins Visier genommen. Dazu kommt die Manipulation von RMM-Software, um geschäftliche E-Mail-Systeme zu kapern oder Ransomware-Angriffe zu verüben. Die Hacker werden diesen neuen Fokus vermutlich beibehalten.

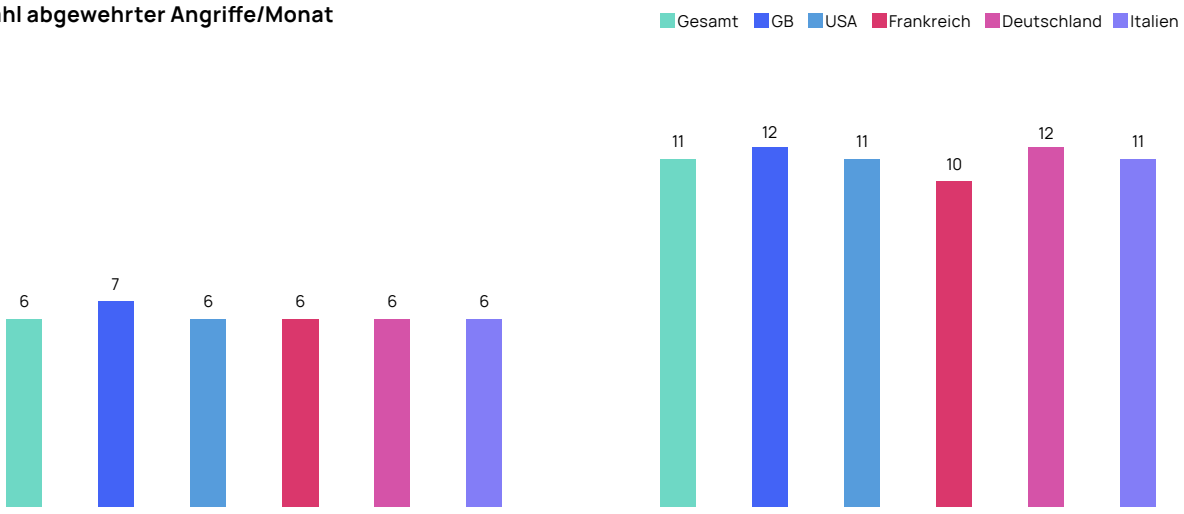
Ein Grund dafür: Zu viele Angriffe auf MSPs verlaufen noch immer erfolgreich. Unsere Umfrage ergab, dass fast alle MSPs in den letzten 18 Monaten Opfer eines Cyberangriffs waren. Und 90 % registrieren mehr Angriffe seit dem Ausbruch der Corona-Pandemie. Ein Drittel der erfolgreichen Angriffe fiel alleine in das letzte Quartal. Und: Die Anzahl der von MSPs abgewehrten Angriffe hat sich fast verdoppelt: von 6 auf 11.



9/10 MSPs

90 % der MSPs registrieren mehr Angriffe seit dem Ausbruch der Corona-Pandemie.

Anzahl abgewehrter Angriffe/Monat



Durchschnittliche Angriffe pro Monat **vor** der Pandemie

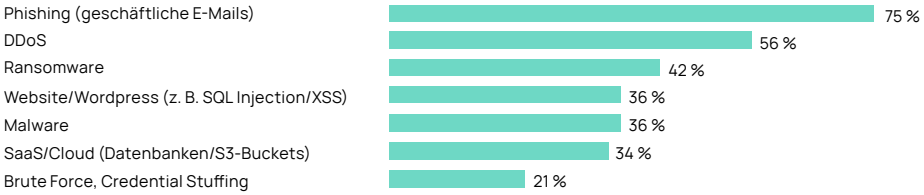
Durchschnittliche Angriffe pro Monat **seit** der Pandemie

Nur eine Antwortmöglichkeit pro Frage

Befragte, die eine Zunahme von Cyberangriffen festgestellt haben: Gesamtstichprobe (451) Großbritannien (86) USA (85) Frankreich (92) Deutschland (90) Italien (98)

Angriffe und Angriffsvektoren

Angriffsformen nach Häufigkeit



Die befragten MSPs registrieren (mit regionalen Abweichungen) eine starke Zunahme von drei Angriffsmethoden:

1. PHISHING

Phishing ist der beliebteste Angriffsvektor, am häufigsten genannt in Italien (86 %) und Frankreich (82 %).

2. DDOS

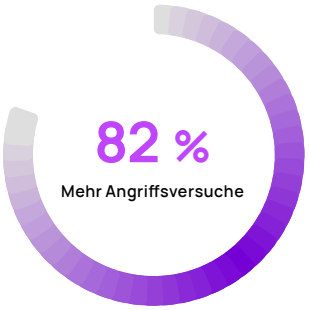
DDoS-Angriffe sind besonders in den USA auf dem Vormarsch (65 %).

3. RANSOMWARE

55 % der US-amerikanischen MSPs werden häufig mit Ransomware angegriffen (Großbritannien: nur 34 % der MSPs). Das passt ins Bild der aktuellen großen Cyberangriffe.

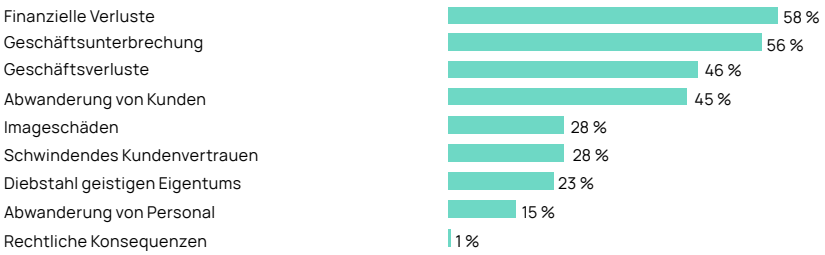
Mangelhafte Sicherheit hat Folgen

Den befragten MSPs zufolge haben bei 82 % ihrer Kunden Angriffsversuche zugenommen. Seit der Pandemie wurden durchschnittlich 14 Angriffe pro Monat verhindert, vor der Pandemie lag dieser Wert noch bei 8 Angriffen pro Monat.



Cyberangriffe haben verheerende Auswirkungen auf MSPs und die von ihnen betreuten Unternehmen. Die Folgen sind abwandernde Kunden, finanzielle Verluste und Geschäftsunterbrechungen.

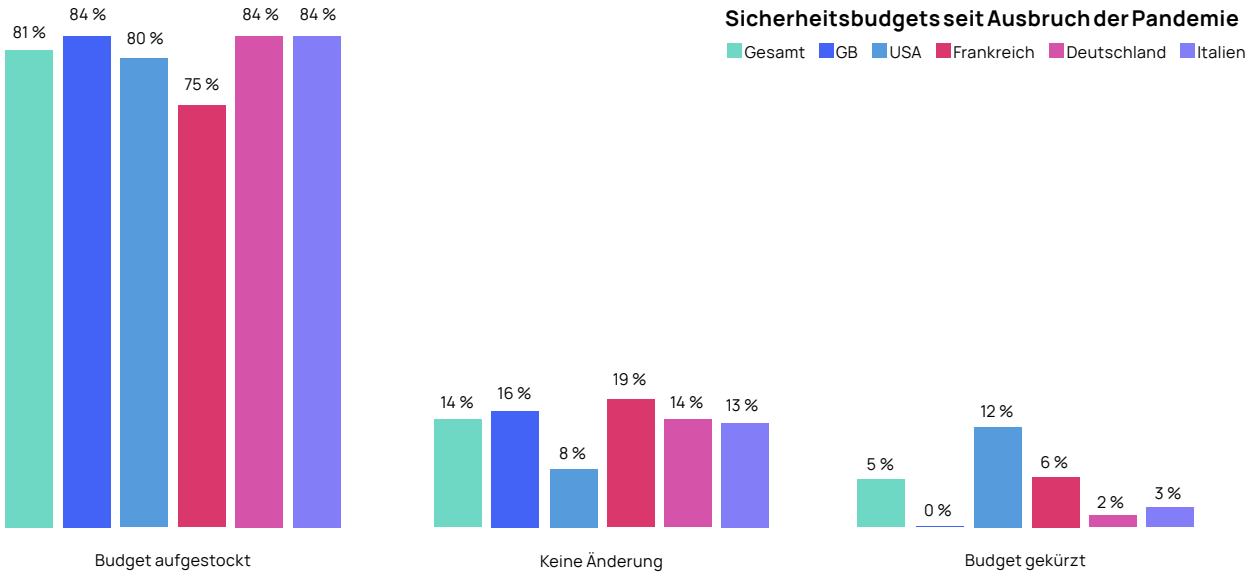
Geschäftliche Folgen von Cyberangriffen



Wie unsere Umfrage zeigt, ist die Abwanderung von Kunden besonders in Frankreich und den USA ein Thema. In Italien ist es eher das schwindende Kundenvertrauen. Die stärkste Mitarbeiterabwanderung aufgrund eines Angriffs verzeichnen Kunden deutscher und britischer MSPs, nämlich 26 %.

MSPs passen sich an die schwierigen Bedingungen an

Die Lage ist bedrohlich, doch die MSPs rüsten auf. 4 von 5 der von uns Befragten stocken ihr Sicherheitsbudget auf (Frankreich: 3 von 4). Aufgestockt wird durchschnittlich um 5 %; **in Frankreich einen Prozentpunkt weniger, in Deutschland einen mehr.** Ob dies angesichts nahezu verdoppelter Angriffszahlen auf MSPs ausreicht, bleibt abzuwarten.



81 % der MSPs haben ihr Sicherheitsbudget im Zuge der Pandemie aufgestockt; bei ihren Kunden liegt dieser Wert bei 70 %. Wie oben beschrieben, haben KMU ihre Budgets um ganze 7 % erhöht. MSPs wären durchaus gut beraten, vergleichbar stark aufzustocken, um Schritt zu halten.

Wofür geben MSPs ihr Geld aus?

Ihr Budgetplus investieren MSPs vor allem in Datensicherheit, Cloud-Sicherheit und Absicherung der Infrastruktur. Am wenigsten wenden sie für Identität und Zugriff auf. MSPs setzen die Mittel unter anderem für Datenverschlüsselung, AV und Multifaktor-Authentifizierung ein. Interessant sind die Unterschiede von Land zu Land: MSPs in Frankreich investieren eher in VPNs, während in Großbritannien und Deutschland mehr Geld in E-Mail-Filterung fließt.

Grundbausteine schaffen Sicherheit

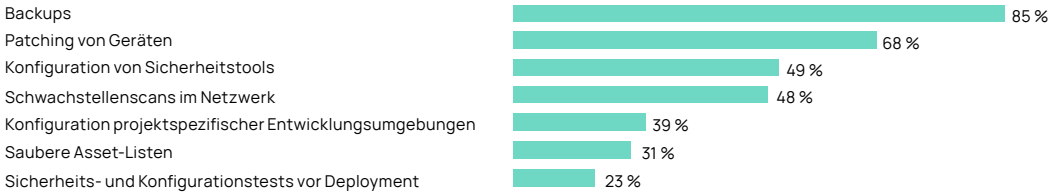
Für den Schutz ihrer Kunden brauchen MSPs ganz bestimmte Grundbausteine, die jedoch noch nicht bei allen ausreichend Beachtung finden.

1. AUTOMATISIERUNG IST DAS A UND O

Angriffe nehmen zu und werden immer raffinierter. Eine manuelle Abwehr ist heutzutage quasi nicht mehr möglich. Wer den Geschäftsbetrieb seiner Kunden besser schützen möchte, muss deshalb automatisieren. Aktuelle Beobachtungen in der Branche:

- **Backups** sind der Bereich, in dem MSPs am häufigsten automatisieren, um den Geschäftsbetrieb ihrer Kunden abzusichern – 85 % aller Befragten insgesamt, in Frankreich und Italien sogar über 90 %.

Automatisierung zum Schutz des Kundenbetriebs



- **Patching** – 80 % der MSPs spielen Patches automatisch ein.
- **Webfilter** – 90 % der MSPs nutzen automatische Webfilter, in der Regel URL-basiert. Nur etwa 10 % nutzen die sicherere DNS-Filterung.
- **Sicherheits- und Konfigurationstests vor dem Deployment** werden aktuell von weniger als einem Viertel der MSPs automatisch durchgeführt.

2. BACKUP IST WICHTIG – MIT DER RICHTIGEN TAKTUNG

Backup ist bei einem Angriff die letzte Verteidigungslinie: MSPs müssen im Ernstfall Kundendaten und -systeme jederzeit wiederherstellen können. Die meisten Kunden erhalten Backup-Dienste durch ihre MSPs. Doch nur 40 % der MSPs führen Backups von Workstations alle 48 Stunden oder häufiger durch. In Frankreich ist dieser Wert mit 60 % höher. Bei Servern sieht es insgesamt besser aus: 74 % der MSPs machen hier alle 48 Stunden Backups.

Immer mehr Geschäftsprozesse werden in die Cloud verlagert. Einen Backup von Microsoft-365™-Daten bieten die meisten MSPs inzwischen an. Die Spanne reicht von 100 % der MSPs in den USA bis hin zu 87 % in Deutschland.

> „Fast alle MSPs bieten Microsoft-365-Backups an.“

3. STIEFKIND MULTIFAKTOR-AUTHENTIFIZIERUNG

Fast alle MSPs bieten ihren Kunden Zwei-Faktor-Authentifizierung (2FA) an, nur 40 % haben sie jedoch selbst implementiert. Auch von den Kunden nutzt aktuell nur ein Drittel 2FA. Allerdings sagen die Befragten, dass sie in den nächsten fünf Jahren 95 % der Kunden auf 2FA umstellen möchten, den Großteil davon in den nächsten beiden Jahren.

Obwohl Identity Management ein zentraler Sicherheitsbaustein ist, hat es weder bei MSPs noch bei ihren Kunden einen hohen Stellenwert. Bei aller Kundenorientiertheit sollten MSPs die mühsame, aber notwendige Aufklärungsarbeit dazu nicht scheuen.

„Nur ein Drittel der Kunden nutzt aktuell 2FA.“

EINFÜHRUNG VON 2FA

2021 **2026**

33 % → **95 %**

Gesetzliche Vorgaben für MSPs zur Cybersicherheit

Die globale Security-Landschaft ist gerade stark im Wandel. Das betrifft ganz besonders MSPs. Das zwischen Frankreich und den USA geschlossene Cybersicherheitsabkommen verleiht dem globalen Cyberdialog auf staatlicher Ebene Schub. Mehrere gezielte Supply-Chain-Angriffe im Jahr 2021 haben zu einer engeren Zusammenarbeit zwischen Technologieanbietern, IT-Serviceanbietern und staatlichen Institutionen geführt.

Die Bedrohung der Supply Chain durch Angriffe auf MSPs war 2021 so groß, dass verschiedene Staaten nun beschlossen haben zu handeln. So hat beispielsweise die britische Regierung eine Initiative für mehr Cybersicherheit digitaler Supply Chains angestoßen. Sie begründet diesen Schritt damit, dass es „einer stärkeren Intervention bedarf, wenn sich die Resilienz digitaler Supply Chains verbessern soll. Unter allen denkbaren Maßnahmen ist Regulierung aus Sicht der meisten Befragten die wirksamste.“[2]

In erster Linie sollen nun gesetzliche Vorgaben erarbeitet werden, die sicherstellen, dass MSPs „vernünftige und angemessene Cybersicherheitsmaßnahmen“ treffen.

Dies könnte im Klartext bedeuten, dass MSPs bestimmte Cybersicherheitspraktiken einhalten müssen, etwa Richtlinien für den Schutz von Geräten vor unbefugten Zugriffen, oder sie für die At-Rest- und In-Transit-Verschlüsselung von Daten sorgen müssen. Es könnte weiterhin bedeuten, dass sie Backups sicher und zugänglich vorhalten, Mitarbeiter schulen und sich um die Entwicklung einer gesunden Cybersicherheitskultur kümmern müssen.

[2] https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security

Fazit

MSPs sind die stillen Helden der Pandemie und sollten Sicherheit jetzt zu ihren Gunsten nutzen

Viele MSPs haben in der Pandemie den Geschäftsbetrieb ihrer Kunden zuverlässig am Laufen gehalten und ihnen bei der Umstellung auf den Homeoffice-Betrieb geholfen. Sie haben internen IT-Teams unter die Arme gegriffen, besonders dann, wenn diese ihre Sicherheitsprofis abordern mussten, um Endbenutzern Homeoffice-Support zu geben. Den unschätzbaren Wert ihrer Leistung haben MSPs in der Pandemie auf vielerlei Weise gezeigt.[3]

Allerdings sollten MSPs das Vertrauen, das man ihnen während der Pandemie entgegengebracht hat, nun nicht leichtfertig verspielen, indem sie beim Schutz ihrer eigenen Systeme nachlässig sind. Fakt ist, dass sie heute stärker im Visier von Kriminellen und denselben Gefahren wie ihre Kunden ausgesetzt sind. Viele MSPs stocken bereits ihr Sicherheitsbudget auf und investieren in neue Tools. Doch was sie tun, ist möglicherweise zu wenig, um der zunehmenden Angriffe Herr zu werden.

Angesichts der sich andeutenden gesetzlichen Regulierungen ist ein Fokus auf die Grundbausteine der Cybersicherheit wichtig. Bei ihren Kunden sprechen MSPs diese durchaus an. Doch es ist wichtig, dass sie mit gutem Beispiel vorangehen und Technik, die sie ihren Kunden anbieten, auch im eigenen Betrieb einsetzen. Unsere Umfrage zeigt, dass MFA, häufigere Backups und eine stärkere Automatisierung die Knackpunkte sind.

Die gute Nachricht: Viele MSP-Kunden müssen gar nicht von Sicherheitsinvestitionen überzeugt werden. Sie stocken ihre eigenen Sicherheitsbudgets bereits auf und haben klare Prioritäten, wofür sie das Geld ausgeben möchten. Wichtig ist, dass MSPs ihre Rolle als zuverlässiger Partner und Berater weiter ausüben und bei ihren Kunden und sich selbst für die erforderliche Sicherheit sorgen.

[3] „(ISC)² Survey Finds Cybersecurity Professionals Being Repurposed During COVID-19 Pandemic“ (isc2.org)

Anmerkung: Alle im Dokument genannten Zahlen basieren auf den Ergebnissen der unabhängigen Umfrage im Auftrag von N-able.