Digital Security
Progress. Protected.

MANAGED SECURITY SERVICES:

Ein Wegweiser für KMU

Sicherlich kennen Sie dieses Problem: Ihre Administratoren arbeiten täglich bis zum Anschlag. Sie haben von der optimierten Netzwerkperformance bis hin zum vergessenen Passwort mehr als alle Hände voll zu tun. Und dann sollen sie sich auch noch um eine perfekte IT-Sicherheit kümmern? Managed Service Provider könnten helfen, den gordischen Knoten zu zerschlagen.

Inhaltsverzeichnis:

Kapitel 1
Die neue Rolle von MSP/MSSP

Die IT in Unternehmen wird immer komplexer, Fachkräfte immer rarer und Cyberangriffe immer raffinierter. Diese Gemengelage bereitet Unternehmen immer mehr Kopfzerbrechen. Während größere Firmen oftmals auf eine eigene IT-Abteilung zurückgreifen können, standen KMU und Kleinbetriebe vor einem echten Dilemma. Alleine schafften sie es kaum, das eigene Netzwerk sicher vor Cyberkriminellen zu schützen. Das Outsourcen an spezielle Dienstleister war aufwändig und kostspielig.

So wundert es nicht, dass sogenannte Managed Services gerade für diese Unternehmen eine attraktive Option darstellen. Dabei handelt es sich um IT-Dienstleistungen, die von IT-Fachhändlern, Systemhäusern und spezialisierten Security-Unternehmen angeboten werden.

Ganz neu ist die Idee der Managed Services nicht. Sie haben bereits Mitte der Nullerjahre schnell an Bedeutung gewonnen. Mit dem Angebot an diversen Leistungen haben einige Systemhäuser ihr klassisches Geschäftsfeld rund um IT-Consulting und Vorortbetrieb von Hard- und Software erweitert. So können sie ihren Kunden als Managed Service Provider (MSP) ein erweitertes Portfolio rund um IT-Lösungen anbieten.

Dabei sind Managed Services weit mehr als das pure Bereitstellen schlüsselfertiger Lösungen. Im Idealfall stellt ein MSP Anwendungen und Lösungen nach dem exakten Bedarf eines Unternehmens bereit, kümmert sich um deren Betrieb und passt sie kontinuierlich neuen Anforderungen an. Auch das Aufspielen von Updates, die Einbindung neuer Hardware und die Sicherung der Datenintegrität zählen zu den Aufgaben der Experten.

Heute setzen immer mehr Unternehmen fast jeder Größe auf MSP. Vom kleinen Mittelständler, der über keine eigene IT-Abteilung verfügt, bis hin zu Großunternehmen, die für Spezial-Lösungen auf externe Kompetenz setzen. Fast immer steht hinter der Nutzung der Wunsch, die eigene IT-Abteilung zu entlasten. Mittlerweile umfasst eine Unternehmens-IT viele verschiedene Technologiefelder wie Netzwerkmanagement, gesetzeskonforme Datensicherungen, dedizierte ERP-Lösungen, integrierte Kommunikationslösungen und Security. Selbst eine größere IT-Abteilung in einem Unternehmen stößt an ihre Grenzen, wenn es um spezielle Lösungen geht. Managed Service Provider verfügen in der Regel über hohe Expertise in ihren Spezialgebieten und sorgen dafür, dass die eingesetzten Lösungen immer dem aktuellen Stand entsprechen. Zudem ist es für Firmen immer schwieriger, geeignete IT-Experten zu finden.

Laut einer Analyse des Digitalverbands Bitkom blieben 2021 hierzulande 96.000 solcher Stellen unbesetzt. Ein Ende dieses Fachkräftemangels ist nicht in Sicht.

Insbesondere im Hinblick auf IT-Sicherheit ist die Experten-Unterstützung jedoch mehr als sinnvoll. Die höchst angespannte und immer komplexer werdende IT-Bedrohungslage erfordert eine hohe Aufmerksamkeit und detaillierte Kenntnisse im Bereich Security.

Der aktuellen IDC Studie „Cybersecurity in Deutschland 2021“ zufolge haben Unternehmen in Deutschland mit diversen Problemen zu kämpfen:

- 70% der befragten Unternehmen waren bereits Opfer von Ransomware
- Mit 29% benennt fast ein Drittel der Befragten die vorherrschende und weiter steigende Security-Komplexität als Top-Herausforderung
- Fast die Hälfte der Organisationen beschäftigt sich noch nicht mit „Digital Trust“

IDC hat im September 2021 in Deutschland branchenübergreifend Security-Verantwortliche aus 200 Unternehmen mit mehr als 100 Mitarbeitern befragt, um detaillierte Einblicke in die Herausforderungen, Vorgehensweisen und Pläne beim Aufbau und Betrieb von Security-Landschaften im Kontext allgemeiner IT- und Business-Entwicklungen zu erhalten.

Zusätzlich setzt die Einhaltung des gesetzlich vorgeschriebenen Schutzes der Datenintegrität (Stichwort: EU-Datenschutz-Grundverordnung) Unternehmen unter Druck. Immer mehr Firmen setzen daher in diesem sensiblen Bereich auf externes Know-how. Aufgrund der herausfordernden Vielschichtigkeit des Themas hat sich im Bereich der Managed Services eine eigene Sparte entwickelt, die Managed Security Service Provider – MSSP. Sie bieten Unternehmen das Fachwissen und die Lösungen, um ihre gesamte IT-Infrastruktur vor Angriffen zu schützen und im Extremfall den reibungslosen Betrieb der Geschäftstätigkeit nach einem Sicherheitsvorfall zu gewährleisten.

Kapitel 2
Warum KMU jetzt auf MSP/MSSP setzen

Viele kleine und mittelständische Unternehmen agieren in ihren Geschäftsbereichen hoch dynamisch. In puncto Digitalisierung und vor allem IT-Sicherheit können sie jedoch selten mit größeren Betrieben mithalten. Der Markt mit seiner schnellen Entwicklung nimmt darauf keine Rücksicht, sodass es den KMU zusehends schwerfällt, sich zu behaupten.

Digitalisierungsstau bei KMU

Um sich auf Dauer zukunftsfähig aufzustellen und wettbewerbsfähig zu bleiben, sind mittelständische Unternehmen deshalb darauf angewiesen, ihre Digitalisierung voranzutreiben. Nur so können sie neue, profitable Geschäftsfelder erschließen, die den wirtschaftlichen Fortbestand sichern.

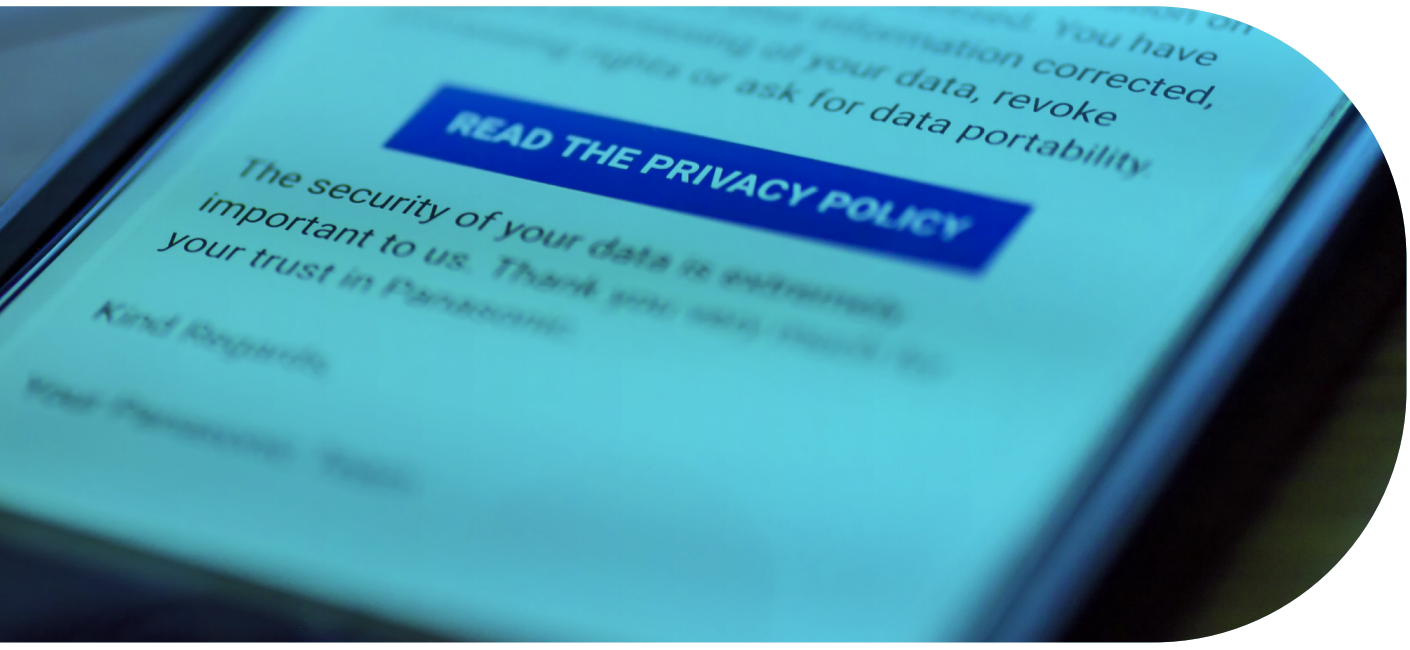
Einfach ist dieses Vorhaben indes nicht: Hürden für die stringente Digitalisierung sind neben finanziellen Mitteln häufig falsche Ansätze, Insellösungen und der Mangel an der nötigen Kompetenz im Hause. Das Fehlen einer Digitalisierungsstrategie steht einem schnellen und reibungslosen Digitalisierungsprozess ebenfalls im Weg. In dieser Ausgangssituation sind erfahrene Dienstleister gefragt, die dem KMU zur Seite stehen: von der Analyse des Ist-Zustands, über ein Pflichtenheft bis hin zur Aufstellung eines Projektplans. So holt sich das Unternehmen von Anfang an entsprechende Expertise ins Haus, um den Gesamtprozess erfolgreich zu initiieren. Es müssen nur zielorientierte Investitionen getätigt werden und es entsteht keine Bindung an teure In-House-Ressourcen.

Den Wandel begleiten

Auch nach der Implementierung von digitalen Prozessen endet der Bedarf an Know-how nicht. Digitalisierung ist ein adaptiver Prozess, der einem Wandel unterworfen ist. Zu einem „Ergebnis“ führen lässt er sich

deshalb nicht. So ist beispielsweise Compliance-Management eine sich stetig ändernde Aufgabe für Unternehmen, bei der immer neue und sich verändernde Regularien und Gesetze berücksichtigt werden müssen. Erschwerend kommt hinzu, dass sie je nach Branche sehr unterschiedlich anwendbar sein und verschiedene Gewichtungen haben können. Den Regeln der EU-Datenschutz-Grundverordnung (DSGVO) müssen alle Firmen gleichermaßen genügen. Die Ende Mai 2018 in Kraft getretene DSGVO ist eine Verordnung der Europäischen Union. Sie regelt die Verarbeitung personenbezogener Daten. Bei Verstößen drohen hohe Strafen. Auch für KMU ist es daher unerlässlich, dass Daten nicht in unbefugte Hände geraten. Gerade in Zeiten von Corona und Homeoffice eine überaus herausfordernde Aufgabe. So haben die ESET Security-Forscher einen deutlichen Anstieg der Angriffe auf die IT-Systeme von Mitarbeitenden im Homeoffice verzeichnet. Eine gefährliche Entwicklung, wenn Cyberkriminelle über etwaige Schwachstellen in Heimbüros in das Firmennetzwerk eindringen und dort auf sensible Daten zugreifen könnten.

MSPs und insbesondere MSSPs besitzen darüber hinaus die notwendige Kompetenz, um bei der Einbindung externer Geräte von Mitarbeitenden und dem damit oft verbundenen Zugriff auf das Firmennetzwerk für die Einhaltung rechtlicher Vorgaben zu sorgen.



Kapitel 3
Vielfältige Bedrohungen – Aufspüren ist der erste Schritt

Gerade kleinen und mittelständischen Unternehmen brennt das Thema Cybersecurity unter den Nägeln, denn sie werden besonders häufig Opfer von Hackerangriffen. Begrenzte Sicherheitsressourcen machen die Firmen zu einer attraktiven Beute für Kriminelle. Gleichzeitig sind die Schäden für diese Unternehmen besonders verheerend. Laut einer Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hatte eine von vier Cyberattacken auf Firmen mit unter 50 Angestellten existenzbedrohende Folgen.

Fest steht: ein einfacher Virenschutz reicht schon lange nicht mehr aus, um alle möglichen Einfallsvektoren zuverlässig abdecken zu können. Als besondere Herausforderung erweist sich die Absicherung von Remote- und Hybrid-Arbeitsumgebungen, die im Zuge der Corona-Pandemie flächendeckend in Deutschland gewachsen sind. Sicherheitsexperten von ESET warnten bereits 2020 davor, dass sich die Anzahl der täglichen Hacker-Angriffe auf Remote Desktop Verbindungen (RDP) im DACH-Raum seit dem Corona-bedingten Umzug in das Homeoffice vervielfacht hat. In 2021 wurden ca. 52 Millionen Attacken innerhalb von 24 Stunden auf die digitale Lebensader zwischen Unternehmen und Mitarbeitern gemessen. Viele dieser Angriffe zielten darauf ab, Ransomware einzuschleusen.

Wertvolle Ressource

Es zeigt sich immer wieder, dass sich Cybersicherheit nicht mit den Bordmitteln der KMU realisieren lässt. Maßnahmen wie ein VPN oder ein Antivirensystem können zwar helfen, reichen aber allein nicht aus. Was in den überwiegenden Fällen fehlt, ist ein schlüssiges Konzept, das die relevanten Schwachstellen in der Infrastruktur identifizieren und bewerten kann. Managed Security Service Provider (MSSP) sind eine wertvolle Ressource für die Unternehmen, denn sie bieten ihnen das nötige Fachwissen und können die erforderlichen Dienste leisten.

Der Fokus auf die IT-Infrastruktur reicht nicht aus

Phishing zählt zu den Cyberbedrohungen, die erst einmal nur sehr wenig mit der IT-Plattform zusammenhängen. Cyberkriminelle senden dazu manipulierte Mails an die Mitarbeitenden eines Unternehmens. Diese Mails enthalten Anhänge oder Links, die Schadcode auf den jeweiligen Client laden. So können Kriminelle den Aufwand eines „Hacks" von Passworten oder Serverzugängen vermeiden. Eine perfidere Methode ist das so genannte Spear-Phishing, bei dem die E-Mails personalisiert auf die angegriffene Person zugeschnitten werden, um sie zu unbedachten und letztlich schädlichen Aktionen zu verleiten. Leider haben die Angreifer damit häufig Erfolg und Angestellte fallen auf solche Mails herein. Auch beim Surfen in sozialen Medien können Anwender in die Falle gehen, indem sie dort versehentlich einen manipulierten Link öffnen und Malware laden. Einige Angriffe finden statt, ohne dass es eine direkte Attacke über die IT-Schiene gibt. So kann ein Benutzer beispielsweise versehentlich sensible Informationen zu freizügig weitergeben oder einer E-Mail den falschen Anhang hinzufügt haben. Durch geschickte soziale Ansprache entlocken Kriminelle Angestellten Informationen über Chats, Mails oder gar das klassische Telefon. Solche Szenarien werden bei der Analyse der Bedrohungslage durch das Systemhaus, das als MSSP fungiert, mit dem Unternehmen geprüft und durchleuchten.

Alles im Blick behalten

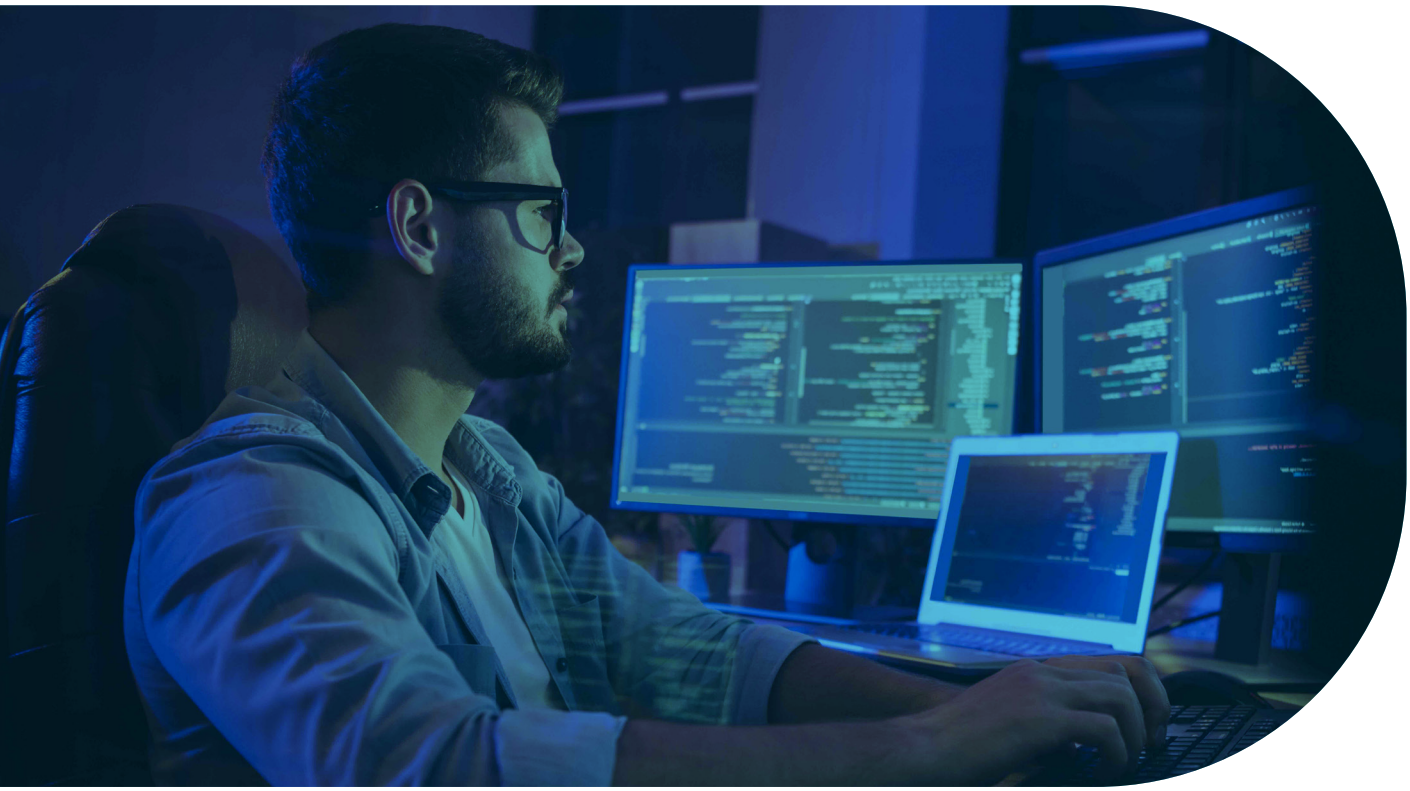
Insider-Angriffe sind ähnlich gelagert, stammen aber vorwiegend aus dem näheren Umfeld eines Unternehmens oder sogar aus dem Kreis der Mitarbeitenden. Die Eindringlinge können auch an den Kunden, Partnern und Zuliefererketten des Unternehmens interessiert sein und es über einen Dienstleister angreifen, was als "Supply-Chain"-Angriff bezeichnet wird. Ein Beispiel dafür ist das so genannte Tailgating, bei dem ein Angreifer unbemerkt durch Sicherheitsschranken hindurchschlüpfen kann. Ein Cyberkrimineller gibt vor, er sei Mitarbeitender eines Lieferanten des jeweiligen Unternehmens und benötige ein bestimmtes Dokument. Der arglose Empfänger beurteilt aufgrund einer gefälschten Sendedomain die E-Mailanfrage dieses „Fake-Lieferanten" als echt und sendet ihm aus diesem Grund vertrauliche Dokumente. Auf diese Weise können vertrauliche oder sogar unternehmenskritische Informationen in falsche Hände geraten.

Auch die „Klassiker" nicht aus dem Auge verlieren

Bei den eher Mitarbeiter-bezogenen Bedrohungen kann der MSP seine Kunden beispielsweise mit Awarenesstrainings unterstützen. Darüber hinaus darf ein Unternehmen jedoch auch die Klassiker der Cyberattacken nicht aus den Augen verlieren. Hier setzt das Systemhaus an und analysiert die Netzwerkstruktur samt Schnittstellen. Das Thema ist insofern sehr vielschichtig, weil alle Endpoints erfasst werden und die Rechte-Bibliotheken überprüft werden müssen. Auch Cloud-Services aller Art bergen viele Gefahren, denen die Experten dank ihrer Erfahrung präventiv entgegensteuern können.

Ein Unternehmen muss sicherstellen, dass es über eine Identitäts- und Zugriffsverwaltungspolitik verfügt, die regelt, wer unter welchen Umständen und aus welchen Gründen Zugang zu welchen Systemen, Daten oder Funktionen haben soll. Das gilt für interne Arbeitsplätze, mobile Arbeitsplätze und externe Zugriffe, beispielsweise von Zulieferern und Kunden. Durch diese Policy wird sichergestellt, dass Kriminellen sich nicht zu leicht unbefugten Zutritt zu einem System verschaffen können. Das kann beispielsweise leicht geschehen, wenn über einen Gastzugang der Zugriff auf sensible Daten möglich ist oder eine Website ein Einfallstor zu einer Datenbank bietet.

Zu den Klassikern gehört ein Virenschutz sowie eine Firewall, die durch restriktive Filterfunktionen nur den Zugriff auf Ressourcen für berechtigte Personen erlaubt. Generell sollte auf VPN-Verbindungen gesetzt werden, sobald Mitarbeiter im Homeoffice oder unterwegs auf die eigenen Server zugreifen möchten. Die Absicherung der Server, Endpoints und Mobilgeräte über spezifische Lösungen sowie Encryption Tools, die bei einem Verlust von Mobilgeräten keinen direkten Zugriff auf die Daten der Festspeicher der Geräte zulassen, muss ebenfalls erfolgen. Letztlich zählt auch eine Multi-Faktor-Authentifizierung zu den Security-Basics moderner Arbeitsplätze. Experten sprechen daher von „Multi Secured Endpoints“, wenn diese von den genannten Sicherheitsfunktionen geschützt werden. Auch regelmäßige Backups sind essenziell, denn sie sind ein einfaches und hoch wirksames Mittel, mit denen Unternehmen nach Datenverlust etwa durch Malware, Hardwareprobleme oder Diebstahl ihre Daten und damit ihre digitale Infrastruktur schnellstmöglich wieder herstellen können.



Kapitel 4
Mit MSSP auf der sicheren Seite

Ein Systemhaus setzt nicht auf einzelne Anwendungen, sondern betrachtet die Situation in einem KMU in seiner Gesamtheit. Jedes Unternehmen und sein Risikopotenzial sind einzigartig. Daher ist eine Erhebung sämtlicher Parameter zur Erstellung einer stringenten Cyber-Security-Strategie der Anfang für einen passgenauen und damit wirksamen Schutz. Nach der Umsetzung diese Strategie bleibt der Security Service Provider das Kompetenzzentrum für alle Belange rund um die Cybersicherheit im Unternehmen. Alle Prozesse werden zentral überwacht und alle Systeme können zentral verwaltet werden.

Schneller als die Angreifer

MSSP sorgen dafür, dass die eingesetzen Sicherheitslösungen aktuell bleiben und ihre Experten sich laufend weiterbilden. Durch diese Kombination gelingt es ihnen in der Regel gut, den Angriffsvektoren von Cyberkriminellen immer einen Schritt voraus zu sein. Ein Fulltime-Job, da Angreifer laufend neue Methoden für ihre Attacken entwickeln. Diesen Entwicklungen können kleine mittelständische Unternehmen kaum etwas entgegensetzen, da der Aufwand sehr hoch ist. Dedizierte Mitarbeitende müssten beschäftigt und laufend geschult werden, damit sie die eingesetzten Lösungen stetig anpassen und updaten können. Ein Systemhaus dagegen verfügt über Tools und Fachkenntnisse und kann seine Threat Intelligence optimal mit seinen IT-Sicherheitslösungen kombinieren. Dadurch wird sichergestellt, dass er seine Kunden vor den neuesten Cyberbedrohungen schützen kann.

Datenschutz berücksichtigen

Nicht zu vernachlässigen ist in diesem Zusammenhang das Thema Datenschutz, da es eng mit der IT-Sicherheit verknüpft ist. Eine Verschlüsselung der Daten bietet zum Beispiel neben der gesetzlich geforderten DSGVO Compliance weitere Vorteile für ein Unternehmen, weil so geschäftskritische Inhalte sehr effizient geschützt werden. Denn wenn wichtige Unternehmensdaten, vertrauliche Informationen über Produkte

oder gar Zugangsdaten zu Produktionseinheiten in falsche Hände geraten, kann dies im kritischsten Fall sogar die Insolvenz für das Unternehmen bedeuten. Außerdem kann fahrlässiger Umgang mit Daten und daraus resultierender Datenverlust mit empfindlichen Strafen belegt werden. Ein Grund mehr, hier auf Experten mit geeigneten Lösungen zu setzen, wie sie durch MSSPs verfügbar sind.

Der wichtige Blick auf das Ganze

Nicht zuletzt ist ein Systemhaus mit Fokus auf Managed Security Services in der Regel auch ein Beratungsexperte, der den Blick auf das Ganze eines Unternehmens hat. Anpassungen in der IT-Struktur, Erweiterungen, neue Technologien und Systeme können schon in der Planungsphase in das Sicherheitskonzept einfließen. Die cloudbasierten Security-Lösungen werden dann zeitgleich mit der Anpassung der Systeme skaliert – ohne dass es zusätzlichen Aufwand in der firmeneigenen IT gibt.

Angestellte „mitnehmen“

Unabhängig von den eingesetzten Technologien ist es jedoch immer erforderlich, dass alle Mitarbeitenden im Unternehmen selbst ein Bewusstsein für mögliche Gefahren entwickeln und sich an Sicherheits-Policies halten. Neben einer passgenauen und aktuellen Sicherheitslösung sind daher Regeln erforderlich, die Mitarbeitende für das Thema Security sensibilisieren und so dabei helfen sollen, den fahrlässigen Umgang mit Daten zu verhindern. MSSPs helfen meist auch in diesem Punkt und beraten ihre Kunden bei der Implementierung und Umsetzung von Sicherheitsrichtlinien im Unternehmen.

Bei der Zusammenarbeit mit einem professionellen Systemhaus profitieren KMU also von der Fachkompetenz des Providers in Verbindung mit dedizierten Herstellerlösungen. Die gesamte Komplexität der IT-Infrastruktur wird erfasst und gesichert. Die Lösungen, die ein MSSP für seine Kunden auswählt, werden mit der Kompetenz des Service Providers betrieben. Kleine Unternehmen und Mittelständler erweitern damit ihre IT-Abteilung um dedizierte Sicherheitsexperten, die - je nach Service Level Agreement – einen 24/7 Service bieten und damit einen Rundumschutz garantieren.

Zuverlässiger Partner

ESET ist bereits seit Jahren zuverlässiger Partner für MSSPs. Mit ESET PROTECT hat ESET eine moderne Managementkonsole für MSSPs entwickelt, mit der sie ihrer Aufgabe als Sicherheitszentrale für Unternehmenskunden zuverlässig On-Premises und und mit ESET PROTECT Cloud auch von überall auf der Welt nachgehen können. Es steuert und überwacht das komplette Sicherheitsmanagement für die jeweiligen Kunden eines Managed Security Service Providers. Neben der Installation von Security-Anwendungen und deren Konfiguration werden Updates durchgeführt und Zugriffsrichtlinien vergeben. So lässt sich beispielsweise durch das Definieren von Profilen frühzeitig verhindern, dass Angestellte durch einen arglosen Klick in einer Mail eine Malware-Seite öffnen.

Kapitel 5
Diese Vorteile bringt der Wechsel

Wenn KMU von einem Investitionsmodell in Hard- und Software zu einem Service-Paket bei einem MSSP wechseln, hat das zusätzliche Vorteile für den Kunden. Neben der immer aktuellen Security-Lösung und den professionellen Dienstleistungen profitieren sie von hoher Skalierbarkeit und vergleichsweise niedrigen Kosten.

Managed Service Provider sind Anbieter von Mehrwertdiensten - sie kümmern sich um Hardware, Software, Implementierung und Support. Gleichzeitig haben sie die Kosten im Blick. Experten mit Fokus auf Sicherheit verfügen über Security Operation Center (SOC) und überwachen die IT-Umgebung ihrer Kunden rund um die Uhr in Echtzeit. Sie verteilen die Kosten für ihr Geschäft auf die gesamte Kundenbasis. Die meisten haben ein Modell entwickelt, das den Wert ihrer Investitionen und deren Nutzungsdauer berücksichtigt. Somit können Unternehmen verschieden Service-Modelle angeboten werden, die in der Regel nicht nur technisch, sondern auch wirtschaftlich attraktiver gestaltet sind als eine vom Unternehmen selbst betriebene On-Premises-Lösung.

Wirtschaftlichkeit

Managed Security Service Provider verfügen über fachkundige, zertifizierte Mitarbeitende, die sich ganz auf die von ihnen verwalteten Cybersicherheitsumgebungen konzentrieren. Die Systemhäuser tätigen die hohen Investitionen, um ihre Serviceangebote zu erstellen und sind für die Rund-um-die-Uhr-Überwachung in Echtzeit verantwortlich.

Kosten im Blick

Darüber hinaus hat das Managed-Services-Modell in Bezug auf die Kosten die Nase vorn. Die Kunden bezahlen nur das, was sie tatsächlich nutzen. In kürzester Zeit wird eine neue Lizenz aufgeschaltet, wenn Mitarbeitende hinzukommen, oder eine Lizenz deaktiviert, wenn jemand das Unternehmen verlässt. Auch das Verschieben von Lizenzen, wenn sie in einer anderen Abteilung benötigt werden, ist möglich. Die Abrechnung

erfolgt tagesaktuell. Die Erweiterungen, Updates oder Neuinstallationen werden in der Regel durchgeführt, ohne dass die Arbeit im Unternehmen unterbrochen wird. Denn anders als eine interne IT-Mannschaft können die externen Experten Updates, Änderungen und Neuimplementierungen dann durchführen, wenn sich der eigne Admin längst zur Nachtruhe begeben hat.

Skalierbar von der Anwendung zu Gesamtlösung

Auch wenn keine vollumfängliche Lösung gewünscht ist, bietet ein MSSP für KMU handfeste Vorteile, wie das Beispiel des Systemhauses und ESET Partners Fachin & Friedrich zeigt. So können Kunden zunächst einmal einzelne Softwarelösungen flexibel aus der Cloud beziehen und einsetzen. Benötigt ein zusätzlicher Client beim Kunden ebenfalls die IT-Security-Lösung, wird einfach eine weitere Lizenz freigeschaltet. Die Performance im Firmennetzwerk und die Hardware-Ausstattung werden von den Experten einfach aus der Ferne überwacht.

Auch Fachin & Friedrich Geschäftsführer Björn Friedrich verzeichnet eine wachsende Zahl von Kunden, die die Betreuung ihrer Unternehmens-IT nach extern vergeben wollen. Für Unternehmens-Kunden sieht er deutliche Vorteile durch Managed Services. Die Techniker können Probleme frühzeitig erkennen und vielfach schon dann helfen, wenn es beim Anwender noch zu keinerlei Störungen kommt. Die systematische Überwachung aller Komponenten des gesamten IT-Systems kann sich dabei selbst für Kleinst-Unternehmen bezahlt machen. So wird beispielsweise kontinuierlich geprüft, ob der Virenschutz noch aktuell ist und gegebenenfalls Updates installiert werden müssen. Um Datenverlusten vorzubeugen, führen die MSSP-Experten zudem regelmäßig Datensicherungen und Wiederherstellungstests durch. So sind Unternehmen stets auf der sicheren Seite.

Professionelle Bestimmung des Status Quo

Vor dem Wechsel zu einem Dienstleister stehen allerdings Ihre IT-Hausaufgaben an. Dazu zählt unter anderem eine Auflistung aller in Ihrem Unternehmen genutzte Hard- und Software. Zudem sollten Sie auch Ihre Erwartungshaltung schriftlich definieren. Dieser Aufwand zahlt sich aber doppelt aus. Zum einen erhalten Sie im Gespräch mit dem Managed Service

Provider eine ausführliche, ungeschönte Ist-Analyse Ihrer IT-Sicherheit. Zum anderen leitet sich daraus eine Bedarfsanalyse und ein Lastenheft ab. Sie wissen dann sehr genau, wo der Schuh drückt und wie man zum optimalen Ergebnis kommt. Dies ist deshalb so wichtig, weil viele Unternehmen ihre eigene IT-Security als viel besser einschätzen, als sie in Wirklichkeit ist. Externe Meinungen haben schon vielen Firmenlenkern in puncto Datensicherheit die Augen geöffnet.

Fazit

Die Unterstützung durch einen MSSP kann also auch in ihrem Unternehmen dazu beitragen, Mitarbeitende zu entlasten, das Sicherheitslevel deutlich zu heben und damit auch im Bereich Digitalisierung erfolgreich zu sein.

Diese Vorteile bieten Managed Security Service Provider

- hohe Security-Expertise ohne Bindung von Experten im eigenen Unternehmen
- hochwertige Security-Lösung ohne hohe Investition, stattdessen monatliche Gebühren
- Unternehmen nutzen die Infrastruktur des MSSP mit und sparen
- hohe Flexibilität: Lizenzen lassen sich tagesaktuell anpassen
- die Lösung „wächst“ bei Bedarf mit
- Security-Lösungen werden von den MSSP-Experten kontinuierlich auf dem aktuellen Stand gehalten
- Updates werden durchgeführt, wenn sie den Arbeitsablauf des Unternehmens nicht stören
- Kunden können sich auf ihr Kerngeschäft konzentrieren
- hohe Rechtssicherheit (z.B. DSGVO-Konformität)
- KMU sparen Kosten für die Weiterbildung eigener IT-Experten im Haus

Über ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen. Unsere XDR-Basis mit Endpoint Detection and Response Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ZUFRIEDENE KUNDEN

BVB 09 Champion Partner

Seit 2019 ein starkes Team
auf dem Feld und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel „IT Security made in EU" verliehen

CERTIFIED ISO 9001:2015 COMPANY
CERTIFIED ISO 27001:2013 COMPANY

Unsere Lösungen sind nach Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400k+
Geschützte Unternehmen

200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

welivesecurity by ESET

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH