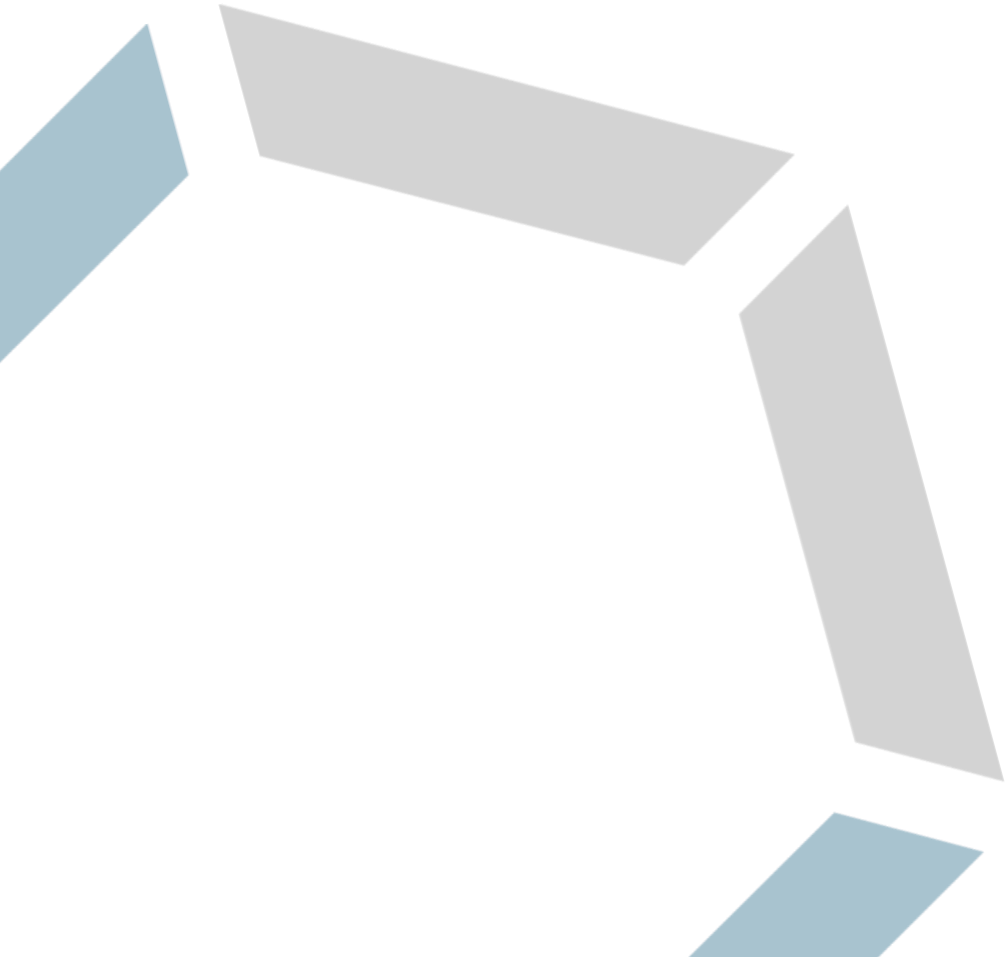
indevis
Sicherheit in einer vernetzten Welt

Whitepaper

5 Tipps, wie Sie IT-Security-Prozesse am besten auslagern



5 Tipps, wie Sie IT-Security-Prozesse am besten auslagern

Für angemessene IT-Sicherheit zu sorgen, wird immer aufwändiger: Die Bedrohungslage wächst, Security-Lösungen werden komplexer, der Fachkräftemangel spitzt sich zu. Viele Unternehmen lagern daher Security-Prozesse an einen spezialisierten Dienstleister aus. In diesem Whitepaper erläutert indevis, worauf Sie dabei achten sollten und woran Sie einen professionellen Service Provider erkennen.

Eben mal die besten Security-Produkte kaufen und in Betrieb nehmen – so einfach funktioniert IT-Sicherheit leider nicht. Die Tools und Lösungen müssen auch richtig zusammenspielen und man muss sie kontinuierlich managen. Das erfordert fundiertes Know-how und entsprechende personelle Ressourcen. Beides ist in Zeiten des Fachkräftemangels schwer zu finden. In vielen Unternehmen arbeiten die IT-Abteilungen ohnehin schon am Rande ihrer Kapazitäten.

Da bleibt kaum Zeit, die zunehmend komplexen Security-Aufgaben zu stemmen. Gleichzeitig werden Cyber-Kriminelle aber immer raffinierter und das Risiko für erfolgreiche Angriffe steigt. Lösen können Unternehmen dieses Dilemma, indem sie IT-Security-Prozesse an einen Managed Security Services Provider (MSSP) auslagern. So profitieren sie von spezialisiertem Know-how, entlasten die IT-Abteilung und können ihr Sicherheitslevel erhöhen.

1. Den richtigen MSSP auswählen

Bei der Wahl des richtigen IT-Security-Dienstleisters sollten sich Unternehmen ausreichend Zeit nehmen und genau hinsehen. Achten Sie auf:

- langjährige Erfahrung des MSSP
- qualifiziertes Personal
- fundiertes Know-how
- Kundenreferenzen
- ISO-Zertifizierungen
- Herstellerpartnerschaften

Der Fokus eines fortschrittlichen Dienstleisters liegt auf der Entwicklung eigener Security-Services auf Basis von Herstellerprodukten. So bietet er Kunden verschiedene Security-Bausteine, aus denen sie genau die auswählen können, die sie benötigen – ohne sich selbst mit den technischen Details auseinandersetzen zu müssen.

2. Gemeinsam individuelle Ziele und Lösungen entwickeln

Ist ein vertrauenswürdiger Partner gefunden, sollte ein durchdachtes Konzept entwickelt werden, das optimal auf die Bedürfnisse des Unternehmens abgestimmt ist.

Die notwendigen Schritte

1. „Kronjuwelen“ identifizieren
2. Was sind die Kerngeschäftsprozesse?
3. Was muss besonders gut geschützt werden?
4. Wie ist der aktuelle Status?
5. Wo besteht Verbesserungsbedarf?
6. Welche Ziele sind realistisch?
7. Wie lässt sich das angestrebte Schutzniveau am besten erreichen?

Der MSSP

- ➔ Stellt gezielte Fragen
- ➔ Hört zu
- ➔ Entwickelt passgenaue Lösungsvorschläge
- ➔ Behält das große Ganze im Auge
- ➔ Achten darauf, dass neue Tools und Services zusammenpassen und sich in die bestehende Infrastruktur und Betriebsabläufe integrieren lassen

3. Klare interne Strukturen und Prozesse schaffen

Damit ein MSS an die internen Strukturen andocken kann, müssen Unternehmen vorab auch ihre Security-Prozesse unter die Lupe nehmen. Nur wenn es bereits einen klaren Prozess gibt, kann man ihn auch ganz oder teilweise auslagern. Andernfalls muss dieser Prozess erst definiert werden. Außerdem braucht man eine klare Schnittstelle zwischen MSSP und Unternehmen. Auch wenn der Dienstleister der IT-Abteilung viele Aufgaben abnimmt, benötigt er einen Ansprechpartner im Haus. Denn er ist immer abhängig von internen Prozessen und Entscheidungen. Umfassende Security kann nur durch eine partnerschaftliche Zusammenarbeit zwischen MSSP und IT-Abteilung entstehen. Hier gilt das Prinzip der geteilten Verantwortung.

4. Die Rolle der IT-Abteilung neu definieren

Mit der Auslagerung von Security-Prozessen fallen operative Tätigkeiten in der IT-Abteilung weg, Aufgaben verändern sich hin zu einer eher steuernden, koordinativen Rolle.

Nötige Skills der IT-Mitarbeiter:
- Projektmanagement
- Soft Skills

Die IT-Abteilung bildet die Schnittstelle zum MSSP und gewinnt dadurch Zeit, sich intensiver um die Geschäftsentwicklung zu kümmern. Sie sollte sich als Business Enabler der Fachabteilungen verstehen und deren Bedürfnisse möglichst schnell und agil adressieren. Tut sie dies nicht, kann sich gefährliche Schatten-IT entwickeln, da Abteilungen dann unter Umständen in Eigenregie Technologien einführen und diese nicht ausreichend in die IT-Security-Architektur einbetten.

5. Systeme in den Managed Service überführen

Nach der Konzeptions-Phase und der Anpassung von Rollen und Prozessen erfolgt die Transition-Phase. Jetzt müssen die Systeme oder Umgebung des Kunden in den Managed Service überführt werden. Dabei geht der MSSP standardisiert vor und stellt mithilfe von Checklisten sicher, dass hohe Qualitätsstandards eingehalten werden. Aufgrund seiner Erfahrung kennt er mögliche Stolpersteine und setzt Best Practices um. Dabei sollte er trotzdem in der Lage sein, flexibel auf individuelle Bedürfnisse des Kunden einzugehen.

Fazit: Der stete Tropfen höhlt den Stein

Indem Unternehmen Security-Prozesse an einen MSSP auslagern, können sie ihr Schutzniveau erhöhen. Sie sollten sich jedoch bewusst sein, dass es nie hundertprozentige Sicherheit geben wird. Vielmehr geht es darum, Risiken zu minimieren und bestmöglich vorbereitet zu sein. Dafür ist es wichtig, die Security kontinuierlich zu überprüfen. Hat sich die Sicherheitslage verändert? Entsprechen die getroffenen Maßnahmen noch den aktuellen Best Practices? Im Zusammenspiel mit einem erfahrenen MSSP gelingt es am effizientesten, Schutzvorkehrungen immer wieder zu optimieren und ein dauerhaft hohes Sicherheitslevel aufrechtzuerhalten.