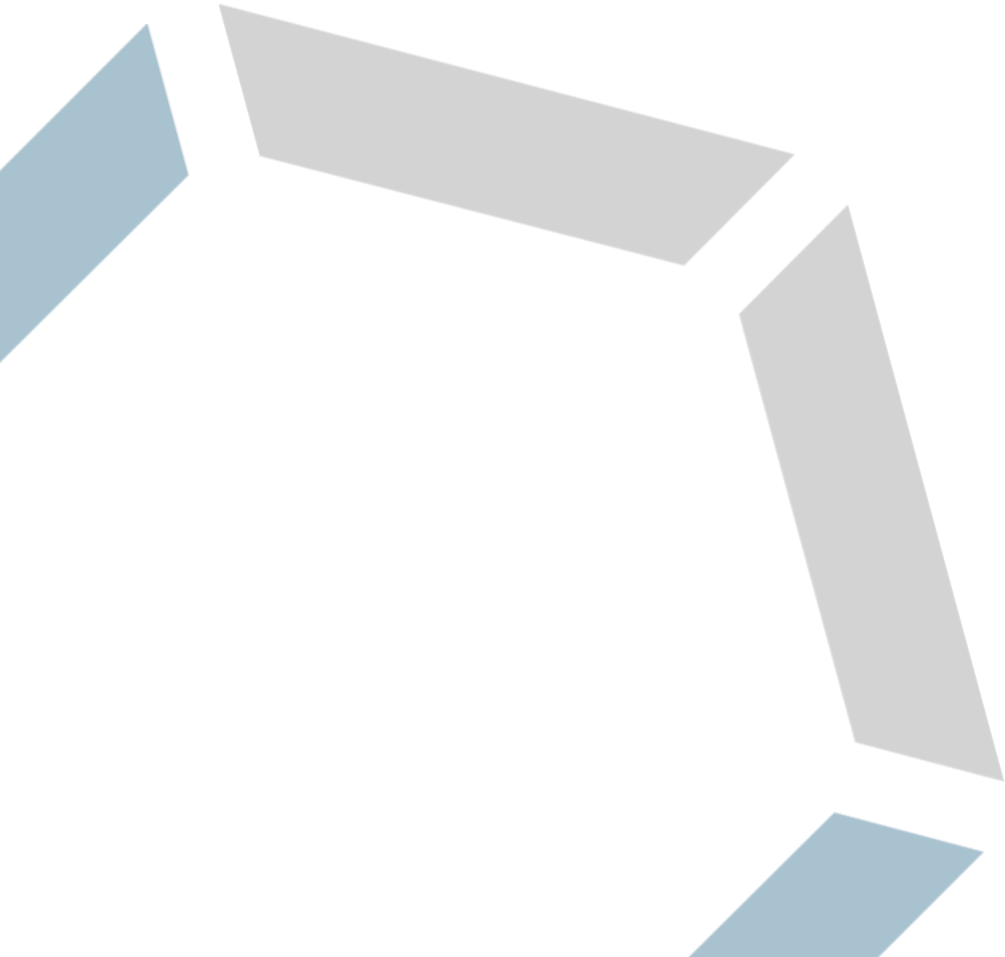
indevis
Sicherheit in einer vernetzten Welt

Whitepaper

6 einfache Schritte zu Ihrem Managed Security Service



6 einfache Schritte zu Ihrem Managed Security Service

Managed Security Services (MSS) sind mehr als nur eine Modeerscheinung, sondern werden von vielen Unternehmen eingesetzt, weil IT-Abteilungen an die Grenzen ihrer Leistungsfähigkeit geraten. Angriffsszenarien wandeln sich stetig, Sicherheitstools werden komplexer und externe Spezialisten können helfen, Risiken, denen Unternehmen in Sachen IT-Sicherheit gegenüberstehen, zu vermeiden. Dieses Whitepaper gibt Ihnen sechs Tipps dazu, was nötig ist, um die Weichen in Richtung MSS zu stellen.

1. Für Grundverständnis sorgen: IT-Sicherheit aus der Steckdose gibt es nicht

Viele Unternehmen wissen, dass sie in IT-Sicherheit investieren müssen und tun dies auch bereitwillig. Um ein Schutzniveau zu erreichen, das seinen Namen auch verdient hat, kann das allerdings nur der erste Schritt sein. Jede IT-Sicherheitslösung muss konfiguriert und in die entsprechenden Betriebsprozesse eingebunden werden. Als Faustregel gilt: IT-Sicherheit besteht aus einem Drittel Technik, einem Drittel Prozesse, Organisation und Schnittstellen sowie aus einem Drittel Benutzer-Awareness. All diese Bereiche müssen berücksichtigt und bedacht werden. Nur dann können sich Unternehmen vor Hackerangriffen bestmöglich schützen. IT-Abteilungen stehen damit grundsätzlich vor der Herausforderung, den Überblick über die vielfältigen Security-Funktionen und -Anwendungen nicht zu verlieren. Sie müssen dafür sorgen, dass die entsprechende Lösung sauber integriert wird und permanent auf dem aktuellsten Stand ist. Das gleicht einer Herkulesaufgabe, die nur die wenigsten Unternehmen intern stemmen können.

2. Strukturen, Prozesse und Verantwortlichkeiten müssen klar definiert werden

Bevor ein externer Dienstleister seine Arbeit aufnehmen kann, ist es entscheidend, dass im Unternehmen Prozesse und Rollen genau definiert werden. Klare Verantwortlichkeiten sind das A und O, wenn beispielsweise bei einer Firewall die Policy geändert werden muss. Denn nur wenn genau festgelegte Abläufe und ein klares Konzept existieren, kann die Basis für Managed Security Services geschaffen werden, die dem Unternehmen auch tatsächlich helfen, die IT-Sicherheit auf Vordermann zu bringen. Sind sich Unternehmen über diese Grundlage nicht sicher, hilft es auch, sich mit dem Managed Security Service Provider einmal zusammenzusetzen und die entsprechenden Grundstrukturen zu erarbeiten. Dabei wird innerhalb von Workshops die Ist-Situation analysiert, um eine Best-Practice-Strategie für die IT-Sicherheit zu entwerfen.

3. Provider machen Inhouse-Experten überflüssig?

Wer bisher alles inhouse erledigt hat, dem fällt es unter Umständen schwer, sich umzustellen und einen externen Experten an seine Heiligtümer heranzulassen. Deshalb müssen die verantwortlichen Mitarbeiter mit an Bord geholt werden. Unternehmen müssen dafür sorgen, dass diese ein Verständnis dafür entwickeln, was ein MSSP leisten und wie dieser unterstützen kann. Alles inhouse zu erledigen ist heute schlichtweg unmöglich. Diese Denkweise sollte daher der Vergangenheit angehören. Vielmehr sollten sich die Mitarbeiter der IT-Abteilungen als „Business Enabler“ für die Fachabteilungen verstehen. Sie müssen die Bedürfnisse ihrer Kollegen in den unterschiedlichen Abteilungen verstehen und die technischen Voraussetzungen dafür schaffen, dass diese mit der Digitalisierung Schritt halten können. Ansonsten droht eine Schatten-IT, die zu gefährlichen Sicherheitslücken führen kann, wenn sich die Fachabteilungen selbst und ohne Rücksprache um ihre IT-Lösungen kümmern. So kann ein gefährlicher, nicht ausreichend geschützter Flickenteppich an Produkten entstehen, der die Angriffsfläche für Hacker vergrößert.

4. Cloud-Migration von Anfang an mitdenken

Im Zuge der Auslagerung von IT-Sicherheit sollte auch gleich das Thema Cloud-Migration mitgedacht werden. Die Sicherheitsmaßnehmen, die Cloud Provider selbst ergreifen, bieten meist nur einen rudimentären Schutz. Das bedeutet: Anwendungen, die vorher in einem historisch gewachsenen und gut gesicherten Ökosystem eingebunden waren, finden sich plötzlich in einer völlig neuen Umgebung ohne wichtige Security-Funktionen wieder. Daher müssen Firewalls zwischengeschaltet werden sowie unter anderem das Zugriffs- und Rechtemanagement definiert und angepasst werden. Auch hier sollten Fachabteilungen, Management und die IT-Abteilung Hand in Hand handeln, sodass Cloud-Services nicht ohne Rücksprache genutzt werden. Die Absicherung von Cloud-Umgebungen ist allerdings aufwendig und erfordert tiefgehendes Wissen über die Technologie des Providers. Ein solches Projekt ist inhouse neben dem Tagesgeschäft kaum zu stemmen. Daher können Managed Security Service Provider auch hier unterstützen, da sie bereits über erprobte Ende-zu-Ende-Lösungen verfügen, mit denen sich Cloud-Umgebungen unkompliziert absichern lassen.

5. Internes Wissen und externe Expertise vereinen

Vielerorts herrscht die Angst vor, die Kontrolle zu verlieren, wenn die IT-Sicherheit an einen externen Dienstleister übergeben wird. Diese Angst ist jedoch unbegründet. Im Gegenteil: Es ist von höchster Bedeutung, dass die interne IT-Abteilung sehr eng mit dem externen Dienstleister zusammenarbeitet. Unternehmensinternen IT-Verantwortlichen kommt dabei eine koordinative, steuernde Rolle zu. Der MSSP ist dagegen vor allem beratend und operativ tätig. Es gilt das Prinzip der geteilten Verantwortung. Es kann nur gelingen, ein hohes Schutzniveau aufzubauen, wenn IT-Abteilungen ihr Wissen über die unternehmensinternen Strukturen und Prozesse teilen. Dieses Wissen kann der MSSP zugrunde legen, um geeignete Security-Tools auszuwählen und auf dieser Basis passgenaue IT-Security Services zu designen, zu implementieren und kontinuierlich anzupassen.

6. Lassen Sie Sorgfalt bei der Auswahl des MSSP walten

Nicht zuletzt sollten Unternehmen bei der Wahl ihres MSSP große Sorgfalt walten lassen. Immerhin handelt es sich um einen hochsensiblen Bereich, der das gesamte Unternehmen absichert. Um festzustellen, ob ein MSSP ein geeigneter Partner ist, sollten Unternehmen diesen vor Ort besuchen, um die verantwortlichen Mitarbeiter kennenzulernen Ein guter MSSP sollte immer dazu in der Lage sein, Fragen zu beantworten. Zudem sollte er für sämtliche operativen, vertraglichen und prozess-begleitenden Rollen gemäß der ITIL-Best-Practices klare Verantwortlichkeiten definiert haben, sowie die Zertifizierung nach ISO 27001 aufweisen. Ist dies der Fall, erfüllt der Provider gültige DSGVO-Security-Standards zum Schutz von Kundendaten.

Fazit: Vorbereitung ist das A und O

Unternehmen müssen sich darüber im Klaren sein, dass Risiken heutzutage an jeder Ecke lauern. Es stellt sich daher nicht die Frage ob, sondern wann Unternehmen einem Cyberangriff ausgesetzt sein werden. Daher ist es entscheidend, sich so gut wie möglich abzusichern und Handlungsrichtlinien für den Ernstfall parat zu haben. Wer gut vorbereitet ist, kann den Schaden möglichst geringhalten oder ihn sogar ganz vermeiden.

© indevis-WP_MSS-6Schritte 07/2021