Das Schweizer Industriemagazin. Seit 1972.

Mit Schnell-zugriff

maschinenbau

Nr. 6 Juni 2016

Security Audit

Fast täglich liest und hört man von Angriffen auf Firmen und Regierungen. Auch der Datendiebstahl bei kleinen und mittleren Unternehmen nimmt stetig zu. Gemäss aktuellem Report von Symantec sind es bereits 50 Prozent aller Angriffe, die auf KMU-Betriebe mit bis zu 2500 Mitarbeitern abzielen.

Eine einzige Schwachstelle kann genügen, und die eigenen Daten sind in den falschen Händen. Ein Ausfall oder gar Datenverlust hat gravierende Folgen für die gesamte Firma. Maschinen und Menschen sind auf die ständig verfügbaren Informationen angewiesen. Daher gilt es, die IT-Umgebung zu schützen, sei dies vor Ausfällen, Datenmanipulation oder Fehlhandlungen.

Ein Security Audit soll dabei aufzeigen, wie es um die eigene IT-Sicherheit steht. Dabei genügt es nicht, nur die technischen Mittel einer Firma zu prüfen. Wichtig sind auch die Organisation und das technische sowie sicherheitsrelevante Wissen in einer Firma.

Anforderungen an ein Security Audit

Wiederholbarkeit

Ein IT-Security Audit sollte keine einmalige Angelegenheit sein. Die IT-Umgebungen ändern sich heutzutage fast täglich. Was heute aktuell ist, ist in einer Woche bereits wieder veraltet. Firmen wachsen, stellen andere Anforderungen an Hardware und Software. Ein Security Audit sollte daher spätestens nach grösseren Veränderungen in der Organisation oder der Technik wiederholt werden. Dabei sollten nicht nur die veränderten oder neu entstandenen Bereiche angeschaut werden. Meistens haben diese Veränderungen auch Auswirkungen auf andere Bereiche. Welche Konsequenzen haben diese? Wurden durch diese Veränderungen neue Schwachstellen geöffnet? Welche Änderungen sind an die Organisation gerichtet (zum Beispiel Notfallplanung, IT-Strategie/IT-Konzepte)? Dies sind nur einige Fragen, die geklärt werden müssen. Das Security Audit sollte dabei so durchgeführt werden, dass es nachvollziehbar ist.

Objektiv, neutral

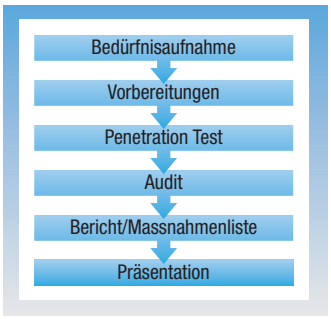
Wichtig bei einem Security Audit ist die Objektivität. Egal durch welche Person eine solche Überprüfung durchgeführt wird, das Resultat sollte das gleiche sein. Diese Anforderung kann nur erfüllt werden, wenn ein standardisiertes Vorgehen gewählt wird. Der Standard ISO 27001 mit seinen Ergänzungen liefert einen idealen Leitfaden. Auch die Grundschutzkataloge des BSI (Bundesamt für Sicherheit in der Informationstechnik) bieten eine umfassende Liste von Kontrollfragen.

Ablauf eines Security Audits

Bedürfnisaufnahme

Die Vorbereitungen auf eine Sicherheitsüberprüfung ist eins der wichtigsten Elemente. Wie sieht die Struktur der zu überprüfenden Firma aus? Welche Mittel werden eingesetzt? Welche Prozesse zeichnen das Unternehmen aus? Sind Verbindungen zu einem externen Arbeitsplatz oder Aussenstellen vorhanden? Gibt es eine IT-Strategie? Welche Anforderungen werden an die Verfügbarkeit, den Datenschutz usw. gestellt?

Mit diesen Fragen kann der Grundkatalog an Fragen und



Ablauf eines IT-Security Audits.

Prüfpunkte vorbereitet werden. Zu klären sind auch Bedürfnisse und Wünsche des Unternehmens. In welche Richtung soll sich das Unternehmen entwickeln? Welche Schwachstellen und Probleme sind bereits bekannt und welche Massnahmen wurden getroffen? Die Geschäftsleitung hat eine einfache Liste mit den kritischen Geschäftsprozessen zu erarbeiten. Die IT-Leitung erweitert die Liste mit den dazugehörenden Applikationen und stellt sicher, dass kritische Systemabhängigkeiten beschrieben werden.

Dokumentation

Bevor ein Audit durchgeführt werden kann, müssen durch die bei der Bedürfnisaufnahme definierten Unterlagen, die Struktur beziehungsweise die Prozesse einer Firma bekannt sein. Fol-

Bild: Archiv

Eine einzige Schwachstelle kann genügen, und die eigenen Daten sind in den falschen Händen.

ZUM AUTOR

Andreas Wisler
goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 320 91 20
www.gosecurity.ch
wisler@gosecurity.ch

gende Unterlagen werden unter anderem geprüft:
- IT-Strategie (eventuell mit Sicherheitskonzept)
- Regelung/Weisungen
- Notfallkonzept
- Technische Unterlagen zu Hardware, Software, Backup und Netzwerkaufbau

Mit der Bedürfnisaufnahme und dem Studium der Dokumentationen können sich die Auditoren sehr gut auf das Unternehmen vorbereiten und kennen die Struktur.

Audit

Damit die Firma komplett untersucht werden kann, empfiehlt sich ein dreiteiliges Vorgehen.

Fragenkatalog

Der Fragenkatalog wird auf Basis der des Standards ISO 27001, den Grundschutzkatalogen des BSI und der Erfahrung der Auditoren erarbeitet. Für jedes Gebiet, technisch oder organisatorisch, werden die Massnahmen zusammengestellt, welche umgesetzt sein müssen, um den gewünschte Sicherheitsstandard zu erreichen. Aus diesen Massnahmen werden die Fragen erarbeitet, über die der Erfüllungstand einer Massnahme festgestellt werden kann.

Die Fragen betreffen alle Stufen einer Firma. Das heisst, es sind Fragen an die Geschäftsleitung (IT-Strategie, IT-Sicherheitskonzept sowie Mitarbeiter- und Notfallplanung), die IT-Verantwortlichen (Hard- und Software, technische Mittel, Backup usw.) sowie die Mitarbeiter (Basiswissen, Sicherheitsverständnis) vorhanden. Die Fragen ergänzen sich teilweise oder ermöglichen eine Rückkontrolle. Dies ist zum Beispiel für Schwächen in der Organisation wichtig. Die Geschäftsleitung ist der Meinung, eine Massnahme wurde sauber umgesetzt, jedoch weiss die IT nichts davon.

Rundgang

Im Rundgang werden die vorhandenen Mittel geprüft. Wie sieht der Serverraum aus? Welche Mittel sind darin vorhanden? Welcher Schutzmassnahmen (Brandschutz, Früherkennung, USV usw.) sind erhalten? Wie ist der physikalische Aufbau des Netzwerkes? Wo werden Backups und Unterlagen aufbewahrt?

Auf dem weiteren Rundgang werden die Arbeitsplätze sowie weitere IT-bezogene Räume untersucht.

Technische Kontrolle

Verschiedene Tools schliessen die Kontrolle der IT ab. Kontrolliert wird, ob die Dokumentationen auf dem korrekten Stand sind, ob Abweichungen vorhanden sind und wie die Konfiguration der Server aussieht (Benutzer, Rechte, Patchstand, bekannte Schwachstellen usw.). Diese Überprüfungen werden nicht nur im internen Netz durchgeführt, sondern auch von Extern. Somit wird auch die Konfiguration der Firewall und der Internetzugänge (VPN) miteinbezogen.

Resultate

Mit den Antworten auf die Fragen werden Rückschlüsse auf bereits umgesetzte oder noch nicht angepackte Massnahmen gezogen. Aus den Massnahmen leiten sich Gefahren ab. Da oft mehrere Massnahmen notwendig sind, eine Gefahr zu beseitigen, ist ein umfangreicher Fragenkatalog notwendig, um Gefahren korrekt einschätzen zu können.

Auswertung

Alle Erkenntnisse aus den verschiedenen Stufen: Dokumentation, externe Kontrolle (Penetration Test), Fragenkatalog, technische Kontrollen und Interviews werden zusammengetragen. Aus diesen Ergebnissen leiten sich Gefahren und entsprechende (Gegen-)Massnahmen ab. Diese werden in einem ausführlichen Bericht festgehalten. Am Ende findet der Kunde eine Checkliste, in welcher alle Massnahmen nochmals kurz aufgelistet und eine erste Gefährdungseinstufung (Gering, Mittel, Hoch) gemacht wird.

Umsetzung

Als Resultat zeigen sich Massnahmen, die umgesetzt werden sollten. Nicht alle Massnahmen sind jedoch kritisch, andere hingegen sehr. Zum Teil haben Massnahmen auch Auswirkungen auf andere Gebiete und Massnahmen. Daher sollte der Umsetzungsreihenfolge grosse Beachtung geschenkt werden. Die Massnahmen sollten nach eigenen Bedürfnissen priorisiert werden. Je grösser die Gefahr, die von einer Lücke ausgeht, umso schneller sollte die Gegenmassnahme ergriffen werden. Die Abhängigkeiten sollten ebenso geprüft und aufgezeichnet werden. Damit eine Massnahme auch umgesetzt werden kann, müssen genügend Ressourcen zur Verfügung stehen. Seien dies finanzielle Mittel, das Wissen oder diejenigen Personen, die alles umsetzen. Mit einem Zeitplan können kritische Lücken schnell angepackt und umgesetzt werden.

Nutzen

Ein IT-Security Audit zeigt pragmatisch und in kurzer Zeit, wie es um die eigene IT-Sicherheit steht. Allfällig vorhandene Schwachstellen in der Infrastruktur können systematisch behoben werden. Durch den detaillierten Bericht sind auch Hintergrundinformationen, warum der Auditor eine Massnahme vorschlägt und welche Massnahmen zur Lösung ergriffen werden können, ersichtlich. Wichtig ist auch, dass der Massnahmenkatalog so aufgebaut ist, dass die notwendigen Schritte selbstständig oder mit dem bestehenden Partner umgesetzt werden können. Somit kann das Unternehmen sicher sein, ihre Kontrollfunktion gewissenhaft wahrgenommen zu haben und optimiert damit die Ausrichtung der Infrastruktur auf die Anforderungen an die Business-Prozesse.