Das IT-Sicherheitskonzept

Gefahr erkannt – Gefahr gebannt?

Die IT-Sicherheit wird immer mehr zu einem Thema. Auch kleinere und mittlere Unternehmen setzen sich mit diesen Fragen rund um die Sicherheit der IT auseinander. Der erste Schritt ist, sich in einem Konzept Gedanken zu machen, was wie und warum geschützt werden muss. Dieser Beitrag basiert auf dem Artikel „Das IT-Sicherheitskonzept" aus der Ausgabe 4/06 und soll Ihnen anhand eines Beispiels zeigen, wie ein solches Konzept für ein mittleres Unternehmen aussehen könnte.

Als Vorlage dient uns das mittlere Unternehmen Baumaterial AG, welches in den letzten Jahren eine kleine Infrastruktur mit drei Servern, 30 Clients und zwei computergesteuerten CNC-Maschinen aufgebaut hat – eine Verbindung zu einem externen Standort und dem Internet ist inzwischen ebenfalls dazu gestossen. Zwei Mitarbeiter sind im Verkauf tätig und können auch von aussen ihre Termine und Adressen abfragen. Die drei Server sind wie folgt aufgeteilt: der erste Server ist der Domain-Kontroller, der zweite Server enthält Exchange, der dritte Server ist die File-Ablage mit einer SQL-Datenbank.

Was will ich schützen?

Die erste Frage gilt dem Schutzbedarf. In einem ersten Schritt geht es darum, herauszufinden, was eines besonderen Schutzes bedarf. Im Falle der Baumaterial AG kann das Unternehmen gut auf die Internetverbindung verzichten, doch wenn die CNC-Maschinen nicht mehr produzieren, können Termine nicht eingehalten werden, was wiederum Einfluss auf die Kundenzufriedenheit hat. Auch sind die vorhandenen Daten von zentraler Bedeutung. Ein Verlust der Daten hat weit reichende Konsequenzen, nicht nur materiell, sondern auch rechtlich.

Die Verfügbarkeit wird in vier Klassen abgestuft: sehr hoch, hoch, gering, sehr gering. Die tolerierbare Ausfalldauer wird in Stunden angegeben. Prioritäten sind nach Möglichkeit aufsteigend zu nummerieren und nicht doppelt zu vergeben. Das wichtigste System trägt die Nummer 1 und das am wenigsten wichtige System die höchste Nummer. Die folgende Tabelle zeigt die Verfügbarkeitsanforderungen an die vorhandenen Mittel:

Objekt	Verantwortlichkeit	Verfügbarkeit Tag / Nacht	Tolerierbare Ausfalldauer Tag /Nacht	Priorität
Domain-Kontroller	IT	Sehr hoch / hoch	4 / 6	3
Exchange-Server	IT	Hoch / Gering	8 / 10	4
File-Server	IT	Sehr hoch / hoch	4 / 6	2
SQL Datenbank	IT	Hoch / Gering	8 / 10	7
CNC-Maschinen	Techniker	Sehr hoch / hoch	4 / 8	1
Internetzugang	Provider	Gering / Sehr gering	8 / 10	8
Zugriff von aussen auf Daten	IT	Hoch / Gering	6 / 10	6
Verbindung zu Aussenstandort	Provider	Hoch / Gering	4 / 10	5

Online-Tipp

Sie haben den ersten Beitrag über das IT-Sicherheitskonzept in der Blickpunkt:KMU Ausgabe 4/2006 verpasst?
Auf www.blickpunktkmu.ch steht der Artikel im Bereich „IT & Kommunikation“ des KMU-Wissensarchivs zum kostenlosen Download bereit.

IT & KOMMUNIKATION

VERFÜGBARKEIT, VERBINDLICHKEIT, VERTRAULICHKEIT

Die drei „V“ im IT-Sicherheitskonzept

Die Grundlagen für jede IT-Umgebung sind ein IT-Konzept und darauf aufbauend ein IT-Sicherheitskonzept. In vielen Firmen findet man ein IT-Konzept, doch das ebenso wichtige Sicherheitspapier fehlt. Dieser Beitrag soll Ihnen zeigen, wie Sie ein IT-Sicherheitskonzept planen und erstellen.

AUTOR: ANDREAS WISLER

Das IT-Sicherheitskonzept beschreibt die notwendigen Massnahmen zur Realisierung und Aufrechterhaltung des für das Unternehmen angemessenen, definierten Sicherheitsniveaus. Darauf basierend kann im Unternehmen ein angemessenes Sicherheitsniveau erreicht und bei konsequenter Durchsetzung der Massnahmen auch gehalten werden. Wichtig ist, das IT-Sicherheitskonzept betrifft alle Stufen. Die Geschäftsführung ist also genau gleich beteiligt, wie die IT-Leitung und die Mitarbeiter.

HINWEIS

Der vorliegende Artikel beschreibt die Grundlagen eines Sicherheitskonzepts. In der nächsten Ausgabe wird Autor Andreas Wisler anhand eines praktischen Anwendungsbeispiels die Umsetzung in der Praxis erläutern.

Drei Beispiele dazu:

Cockpit eines Airbus: Hier ist es von zentraler …

… nimmt hier nur eine nebensächliche Position ein. Der Kontoauszug Ende des Monats ist das verbindliche Papier und wird daher auch im Kleingedruckten geregelt.

Kasse eines Parkhauses: Bei einer Kasse ist die Verbindlichkeit das wichtigste Argument. Es freut sich niemand, wen nach korrekter Bezahlung das Parkhaus doch nicht verlassen kann und die Barriere unten bleibt. Sollte dann doch einmal die Kasse nicht verfügbar sein, steht auch die Schranke offen. Es stört sich auch niemand, wenn der Hintermann …

18 Blickpunkt:KMU 4/2006

Blickpunkt:KMU 4/2006 19

Diese Tabelle kann jederzeit um weitere Mittel wie Telefonanlage, USV, Brandmeldeanlage, Backup, Lagerung von Akten etc. erweitert werden. Ebenfalls können Gruppen gebildet werden, wie zum Beispiel Server, Client, Maschinen, Kommunikation etc.

Wogegen will ich mich schützen?

Die zweite Frage stellt sich, wogegen sich das Unternehmen überhaupt schützen muss. Es muss klar sein, welche Gefährdungen einwirken können und ab welchem Punkt ein Schaden bedrohlich wird. Hier gilt es verschiedene Szenarien und die Folgen abzuschätzen. Ein Beispiel: Die erste Priorität bei der Verfügbarkeit liegt bei den CNC-Maschinen. Stromausfall, Materialschäden, Ausfall eines Mitarbeiters sind Gefahren, die eintreffen und zu einem unmittelbaren Schaden führen können.

Oder nehmen wir den File-Server: Neben Stromausfall, Hardware und Softwareproblemen, kann auch ein Mitarbeiter unkundig Daten löschen. Diese „Gefahren“ sind für alle Objekte in der oben stehenden Tabelle festzustellen. Gegen alle diese Ursachen gilt es sich mit geeigneten Massnahmen zu schützen.

Risikoanalyse

Bevor Massnahmen ausgewählt werden können, gilt es, das Risiko abzuschätzen. Wenn eine „Gefahr“ nur sehr selten eintrifft, ist eine sehr teure Massnahme für ein mittleres Unternehmen nicht angebracht.

Werden Risiken näher betrachtet, so stellt man fest, dass dabei immer betroffene Objekte („was“), Aktivitäten („wie“), Urheber („wer“), eine Motivation („warum“), Häufigkeiten („wie oft“) und ein allenfalls entstehender Schaden („wie viel“) existieren. Gemäss diesen genannten Aspekten können Risiken klassifiziert werden.

Beginnen wir wiederum bei den CNC-Maschinen. In unmittelbarer Nähe der Baumaterial AG steht eine Firma, die Hochleistungsöfen betreibt. Beim Ein- und Ausschalten dieser kommt es zu Spannungsschwankungen. Diese Abweichungen sind auch bei den CNC-Maschinen zu spüren. Der Schaden kann sehr schnell grosse Beträge annehmen, wenn eine Maschine dadurch ausfällt und die Produktion still steht. Das damit verbundene Risiko ist sehr hoch.

„Bevor Massnahmen ausgewählt werden können, gilt es, das Risiko abzuschätzen.“

Bei den Daten auf dem File-Server betrachten wir den Fall des unbedachten Mitarbeiters, der aus irgendwelchen Gründen eine Datei oder ein Verzeichnis löscht – dies kommt bei der Firma Baumaterial AG mindestens einmal pro Woche vor. Die hohe Eintrittswahrscheinlichkeit bedingt entsprechende Massnahmen.

Mini-Glossar

Domain-Kontroller:
Herzstück des Netzwerks, über das alle Benutzerkonten zentral verwaltet werden

Exchange:
Plattform zur Verwaltung von Nachrichten aller Art – vor allem von E-Mails

SQL:
„Structured Query Language“ – Programmiersprache zur einfacheren Verwaltung von Datenbanken

CNC-Maschine:
„Computerized Numerical Control“ – Geräte, die Werkstücke automatisch mit hoher Wiederholgenauigkeit produzieren

USV:
Unterbrechungsfreie Stromversorgung

Massnahmenauswahl

Die Massnahmen, basierend auf der vorhergehenden Risikoanalyse, sollen den eintretenden Schaden minimieren. Oft gehen die Meinungen in diesem Punkt auseinander. IT kostet sonst schon sehr viel Geld und nun kommen weitere Elemente dazu. Es ist jedoch wichtig, alles in Vergleich zu setzen und nicht am falschen Ort zu sparen.

„Nicht alle Risiken können durch technische Massnahmen vermindert oder gar eliminiert werden."

Im Falle der CNC-Maschinen und der Spannungsschwankungen kommen Spannungsregler oder eine umfassende USV-Anlage in Frage. Ob ein Spannungsregler schon ausreicht, muss natürlich abgeklärt werden.

Der File-Server wird durch ein entsprechendes Backup-System gesichert. Werden Daten gelöscht, können diese einfach und schnell wiederhergestellt werden. Die Art des Backups, die Anzahl der Sicherung, die Lagerung der Medien usw. müssen in der Massnahmenauswahl mitberücksichtigt werden. Nicht alle Risiken können durch technische Massnahmen vermindert oder gar eliminiert werden. Hier müssen schriftliche Policies ansetzen; Mitarbeitern und eventuell auch Besuchern muss ein Pflichten- und Nachschlagewerk zur Verfügung stehen.

Restrisikobetrachtung

Reichen die für die IT-Sicherheit vorgesehenen Ressourcen an Personal und Finanzmitteln nicht aus, um sämtliche fehlenden Massnahmen umzusetzen, müssen die Massnahmen für die Umsetzung gemäss den Prioritäten vorgenommen werden. Aus der unvollständigen Umsetzung der Massnahmen resultiert jedoch, dass Sicherheitslücken bestehen bleiben. Diese Restrisiken, die durch die mögliche Schadenshöhe und der Einschätzung der Eintrittswahrscheinlichkeit charakterisiert sind, sollten der Leitungsebene zur Genehmigung vorgelegt werden. Es obliegt der Leitungsebene, wahlweise das Budget zu erhöhen oder das Restrisiko zu tragen.

Schlussbemerkung

Mit den oben genannten Punkten kann sich die Baumaterial AG optimal vor Produktions- und Datenverlust schützen.Nehmen Sie sich die Zeit, die Verfügbarkeiten und Risiken genau zu bewerten. Leiten Sie mit diesen Angaben die Massnahmen ab, damit das Risiko so gut wie möglich reduziert werden kann. Es lohnt sich auch, das erstellte Konzept durch eine externe Stelle auf Vollständigkeit und Durchführbarkeit zu kontrollieren, um die Erfassung aller Schritte und Massnahmen sicherzustellen.

Wichtig ist, dass das IT-Sicherheitskonzept regelmässig auf die Vollständigkeit und Aktualität kontrolliert wird. Auch können Risiken sich immer wieder ändern. Nur wer proaktiv reagiert, kann sich vor neuen Gefahren schützen. Planen Sie genügend Zeit ein, denn ein durchdachtes IT-Sicherheitskonzept ist nicht in einem Tag erstellt. ◆

Zum Autor

Andreas Wisler (Tel. 052 320 91 20), Dipl. Ing. FH, CISSP, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produkteneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinander setzt. System Hardening rundet das Portfolio ab.
Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann.
Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.