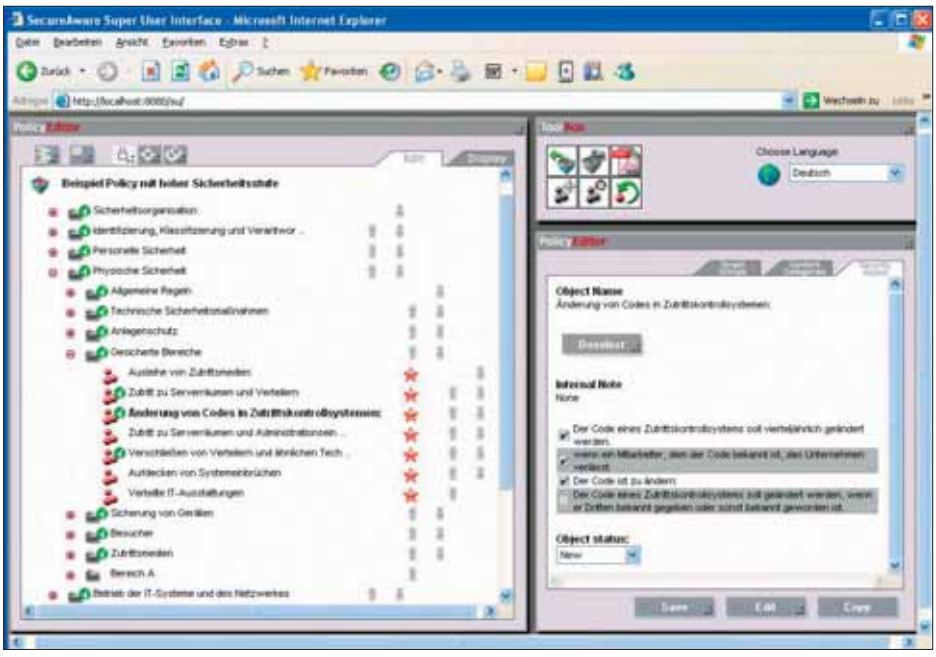
IT-Sicherheitskonzept – Ein Anwendungsbeispiel

Die IT-Sicherheit wird immer mehr zu einem Thema. Auch kleinere und mittlere Unternehmen setzen sich mit 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 1/05 und soll anhand eines Beispieles zeigen, wie ein solches Konzept für ein mittleres Unternehmen aussehen könnte.

VON ANDREAS WISLER*

Als Beispiel 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 dazugestossen. Zwei Mitarbeiter sind im Verkauf tätig und können ihre Termine und Adressen auch von aussen abfragen. Die drei Server sind wie folgt aufgeteilt: Der erste Server ist der Domain-Kontroller, der zweite Server enthält Exchange, und der dritte Server ist die File-Ablage mit einer SQL-Datenbank.

«Ein durchdachtes IT-Sicherheitskonzept ist nicht in einem Tag erstellt.»



Mit dem SecureAware PolicyEditor können Policies mit wenigen Mausklicks zusammengestellt werden.

Was will ich schützen?

Die erste Frage gilt dem Schutzbedarf. Es geht 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 wie folgt abgestuft: sehr hoch, hoch, gering, sehr gering. Die tolerierbare Ausfalldauer wird in Stunden angegeben. Prioritäten sind bei 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 Tabelle unten links zeigt die Verfügbarkeitsanforderungen an die vorhandenen Mittel.

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

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

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.
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.

Zweites Beispiel: Der 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 wird festgestellt, 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.

«Es ist wichtig, alles in Vergleich zu setzen und nicht am falschen Ort zu sparen.»

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 Maschinen zu spüren. Der Schaden kann sehr schnell grosse Beträge annehmen, wenn eine Maschine dadurch ausfällt und die Produktion stillsteht. Das Risiko eines Ausfalles ist hier sehr hoch.

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.

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.

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 Sicherungen und die Lagerung der Medien müssen in der Massnahmenauswahl mitberücksichtigt werden.

Nicht alle Risiken können durch technische Massnahmen vermindert oder gar eliminiert werden. Hier müssen schriftliche Policies ansetzen und den Mitarbeitern oder Besuchern ein Pflichten- und Nachschlagewerk zur Verfügung stellen. Eine Möglichkeit, solche Regelwerke einfach zusammenzustellen, zu verteilen und zu prüfen, ist die Lösung SecureAware der Firma Neupart A/S.

Restrisikobetrachtung

Reichen die für die IT-Sicherheit vorgesehenen Ressourcen an Personal und Finanzmittel 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 die 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, damit Sie wirklich alle Schritte und Massnahmen enthalten.

Wichtig ist, dass das IT-Sicherheitskonzept regelmässig auf die Vollständigkeit und Aktualität kontrolliert wird. Auch können Risiken sich jederzeit 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.

**Andreas Wisler ist Mitglied der Geschäftsleitung der GO OUT Production GmbH mit Sitz in Wiesendangen. Das Unternehmen setzt sich mit IT-Sicherheitsprüfungen und -beratungen auseinander.*