

Virtueller Roundtable „IT-Sicherheitsmanagement im Unternehmen“

Teilnehmer:

Prof. Dr. Norbert Pohlmann

Organisation:

**ifis – Institut für Internet-Sicherheit,
FH Gelsenkirchen**

Kurzeinführung in das Thema:

Die Umfrage des BSI (2004)¹ weist gut funktionierenden IT-Systemen eine wichtige Rolle bei fast 100 Prozent der Befragten zu. Gleichzeitig wird eine mangelnde IT-Sicherheit in den Unternehmen von 89 Prozent der Befragten als erhebliche Bedrohung für die Wirtschaft in Deutschland angesehen.

Die Gefahren steigen weiter: weit vorne liegen Spam und Viren als die größte Bedrohung für die Unternehmensdaten und -informationen. Andererseits wird die Abwehr dieser Bedrohungen auch stärker. Die Unternehmen erweitern ihre IT-Security-Budgets und bauen die IT-Infrastruktur aus. Als Ergebnis wurde im Jahr 2005 bereits bei weniger Unternehmen Schäden wie z.B. Datenverlust oder Systemstörungen gemeldet (von 29 Prozent auf 14 Prozent gesunken) als im Vorjahr. Das IT Sicherheitsmanagement funktioniert also, scheinbar. Oder ist das nur eine Episode im Wettlauf mit den IT-Angriffen, die bald wieder zugunsten der Angreifer ausschlägt?

Welchen Stellenwert hat das IT-Sicherheitsmanagement in den Unternehmen aus der Sicht unserer Experten heute schon oder noch nicht? Wie hoch sollte das Budget für IT-Sicherheitsmaßnahmen sein, woran soll es sich orientieren? Welche Maßnahmen sind „must have“, was ist wünschenswert und wo liegen die häufigsten und wo die gefährlichsten Schwachstellen? Diese und weitere Fragen sind Gegenstand dieser Expertenrunde.

¹ Im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurden 500 Experten, IT-Verantwortliche aus Unternehmen und Verbänden.

Frage 1:

Stellenwert der IT-Sicherheit im Unternehmen

Lange Zeit lag die Verantwortung für die IT-Sicherheit im Unternehmen in den technisch orientierten Abteilungen. Seit längerem wird gefordert, dies zur Chefsache zu machen. Ist dies schon der Fall? Wo liegt Ihrer Meinung nach, die Verantwortung für die Sicherheitsmaßnahmen in einem Unternehmen? Welche Experten sollten das Sicherheitsteam bilden?

Prof. Dr. Norbert Pohlmann:

Wir entwickeln uns in eine Wissens- und Informationsgesellschaft, was bedeutet, dass die Wichtigkeit und die Abhängigkeit der IT immer größer werden.

Damit wird es auch wichtiger, dass die Chefs im Unternehmen die IT als wichtiges und strategisches Instrument verstehen und dementsprechend auch handeln. Die Durchdringung der IT ist in vielen Branchen sehr unterschiedlich und daher auch nicht einfach vergleichbar. Wichtig ist nur, dass es immer notwendiger wird, dass IT-Sicherheit zur Chefsache wird.

Wir alle wissen, dass die IT-Sicherheit nicht nur durch technische Mechanismen wie Firewalls, VPNs, Festplattenverschlüsselung, digitale Signaturen usw. erreicht werden kann. Zusätzlich sind eine klare Zielsetzung des Unternehmens bezüglich der IT-Sicherheit sowie die Aufklärung und die Schulung der Mitarbeiter wichtig, damit alle entsprechend handeln können. Dementsprechend müssen auch die geeigneten Organisationen und Mitarbeiter in den Unternehmen beteiligt werden.

Frage 2:

Grundlagen des IT-Sicherheitsmanagements

IT-Sicherheitsmanagement ist ein weiter Begriff. Die Basics wie Antiviren-Programme, Firewall und Backup-Möglichkeiten gehören bereits zur Grundausstattung jedes Unternehmens. Was ist Ihrer Meinung nach das Kennzeichnende für IT-Sicherheitsmanagement? Was sind unverzichtbare „must have“-Elemente und Maßnahmen? Was sind die wichtigsten Guidelines und Faktoren bei der Auswahl der Sicherheitsmaßnahmen?

Prof. Dr. Norbert Pohlmann:

Ein Kennzeichen für ein IT-Sicherheitsmanagement ist die Bejahung der Frage, ob jeder Mitarbeiter die IT-Sicherheitsziele des Unternehmens kennt und mit den vorhandenen IT-Sicherheitsmaßnahmen umgehen kann, damit diese Ziel erreicht werden können.

Meiner Meinung nach, ist das Wichtigste „must have“-Element angemessene IT-Sicherheitsziele des Unternehmens, die typischerweise mit der Hilfe einer Sicherheitsstudie systematisch erarbeitet werden. Ein zweites wichtiges „must have“-Element ist die Schulung und Aufklärung der Mitarbeiter. Dann müssen für die IT-Gegebenheiten (IT-Ausrüstung, Angriffspotential, usw.) und IT-Sicherheitsziele des Unternehmens die richtigen und angemessenen IT-Sicherheitsmaßnahmen umgesetzt werden.

Die Auswahl der Sicherheitsmaßnahmen hängt von den IT-Gegebenheiten, IT-Sicherheitsziele und Budget ab.

Frage 3:

Compliance und IT-Sicherheitsmanagement

Die Compliance-Richtlinien sollen die Unternehmensprozesse, Ressourcen und deren Nutzung und ggf. Missbrauch transparent machen und dadurch vorbeugen. Welche Bedeutung haben diese Richtlinien auf das IT-Sicherheitsmanagement im Unternehmen? Wie spiegelt sich das in der Umsetzung wider?

Prof. Dr. Norbert Pohlmann:

Nur mit Compliance-Richtlinien können Regeln auch eingehalten werden!

Nur wenn Ziele definiert werden, ist ein Unternehmen in der Lage, Regeln zu formulieren, damit diese Ziele auch erreicht werden. Nur wenn diese Regeln alle kennen können, sie befolgt werden. Usw.

Frage 4:

ROI der IT-Sicherheit

Die Sicherheitsmaßnahmen erzeugen im Unternehmen zusätzliche Kosten. Andererseits, können die professionell eingesetzten Sicherheitsinstrumente große Risiken und Schaden für Unternehmen vermeiden. Welche Controlling-Mechanismen, Benchmarks oder etablierte Ursache-Wirkungs-Ketten haben die IT-Verantwortlichen zur Verfügung?

Prof. Dr. Norbert Pohlmann:

ROI oder besser ROSI (Return on Security Investment) ist ein wichtiger Punkt, da es hilft eine Investition in IT-Sicherheit rational umzusetzen.

Das größte Problem liegt in der Bewertung der potentiellen Schäden und in der Beurteilung der Eintrittswahrscheinlichkeit, dass ein solcher Schaden eintritt. Außerdem ist es eine große Herausforderung, konkrete Angriffe auf IT-Sicherheitsmaßnahmen und IT-Sicherheitsmaßnahmen auf Schäden abzubilden. Das macht es wiederum schwierig, eine ROSI-Berechnung für eine Investition durchzuführen.

Wichtig hier ist, dass die Unternehmen aufgetretene Schäden analysieren und gut dokumentieren, damit diese Erfahrungen für zukünftige Bewertungen zur Verfügung stehen. In diesem Bereich stehen leider keine angemessenen Instrumente zur Verfügung.

Frage 5:

IT-Risiken in einem Unternehmen

Datenbanken, Web-Applikationen, Betriebssystem und vieles mehr sollen geschützt werden. Wo liegen Ihrer Meinung nach die größten Schwachstellen in der IT-Infrastruktur in den Unternehmen? Sind das typische Schwachstellen, die von der Unternehmensgröße oder Branche abhängen oder gibt es globale Fehlerquellen?

Prof. Dr. Norbert Pohlmann:

Eines der größten Probleme ist, dass die Softwarehersteller zurzeit Lösungen zur Verfügung stellen, die zu viele Fehler aufweisen und für Angriffe ausgenutzt werden. Das praktisch nicht vorhanden sein einer Produkthaftung für Software zeigt, dass wir noch im Steinzeitalter sind.

Es gibt einige Initiativen im Bereich Trusted Computing, die sicherlich ein neues Zeitalter einläuten werden (siehe www.emscb.org).

In Abhängigkeit der Wichtigkeit der IT für das Unternehmen und für Branchen gibt es natürlich unterschiedliche Angriffe und Angriffspotential und damit auch andere Notwendigkeiten, sich zu schützen.

Frage 6:

Outsourcing der IT-Sicherheit

Wann ist Outsourcing effizient und in welchen Feldern der IT-Sicherheit überhaupt nur möglich? Welche Anforderungen sollten an Outsourcing-Partner gestellt werden? Haben Sie hier Erfahrungswerte oder Hinweise auf Erfolgsfaktoren für IT-Sicherheits-Outsourcing?

Prof. Dr. Norbert Pohlmann:

Für die meisten kleineren Unternehmen ist IT-Sicherheits-Outsourcing insbesondere im Bereich BackUp und Archivierung ein großes Thema, da es aus der Sicht der Finanzierbarkeit eine interessante Möglichkeit darstellt.

Zusätzlich gibt es im Bereich der Kommunikation zunehmend Angebote wie VPN, die für eine vertrauliche Kommunikation zwischen Unternehmensteilen oder E-Mail Lösungen, die das Viren- und Spam-Problem lösen in breiter Umsetzung.

Welche Anforderungen sollten an Outsourcing-Partner gestellt werden?

Outsourcing-Partner müssen vertrauenswürdig sein. Die Vertrauenswürdigkeit abzuschätzen ist eine nicht einfache Aufgabe. Kriterien können sein:

Aus welchem Land kommt das Unternehmen?

Wie sehen die Verträge aus?

Unter welchem Recht stehen die Verträge?

Welche anderen Firmen sind schon Kunden

Gibt es eine Evaluierung/Zertifizierung des Prozesses?

Usw.

Frage 7:

Trends und Zukunftsentwicklung der IT-Sicherheitsmanagements in Unternehmen

Wie schätzen Sie die weitere Entwicklung der IT-Sicherheit im Unternehmen? Inwieweit sind Trends der Automatisierung und der Integration von Lösungen hier maßgeblich?

Wie sind die Sicherheitsmaßnahmen in Ihrem Unternehmen organisiert? Welche Lösungen bietet Ihr Unternehmen an bzw. welchen Nutzen und Vorteile sehen Sie hier für die Unternehmen?

Prof. Dr. Norbert Pohlmann:

Ich glaube, dass es zunehmend wichtiger sein wird, eine Übersicht über den aktuellen Zustand der Sicherheit in einem Unternehmen zu haben.

Hier sind geeignete Darstellungsformen gefragt, die es uns ermöglichen, in intuitiver und verständlicher Form den aktuellen Zustand zu erfassen.

Zusätzlich sind Mechanismen notwendig, die automatisiert Benachrichtigungen beim Auftreten ungewöhnlicher Ereignisse melden.

Vielen Dank für Ihre Teilnahme!