Vierter qSkills Security Summit. Ein Rückblick

Vom Feind auf leisen Sohlen und anderen Risiken

Laut einer Studie der Beratungsgesellschaft Ernst & Young zum Thema „Datenklau“ unter 400 deutschen Unternehmen, sehen sich über 80 Prozent der befragten Führungskräfte auf der sicheren Seite in puncto Wirksamkeit ihrer präventiven Maßnahmen. Dass dieses Ergebnis verwundert, zu diesem Schluss kommen nicht nur die Macher der Studie, sondern auch Thomas Königshofen, Konzern-Sicherheitsbevollmächtigter der Deutschen Telekom AG. Im Rahmen des vierten qSkills Security Summit, am 10. Oktober 2011 in Nürnberg, zeigten Königshofen und weitere Experten aus dem Security- und Riskumfeld praxisnahe Wege zu mehr Sicherheit und Sensibilität im Umgang mit der Ware Nummer eins: Informationen.

Datendiebstahl: bekannt und doch unterschätzt

Schaut man sich die Bandbreite potenzieller Gefahrenszenarien an, rangieren Naturkatastrophen vor dem Terrorismus und dem organisierten Verbrechen. Das Thema Datendiebstahl steht nach den Worten Königshofens dagegen noch immer am Ende des „Level of violance“. Warum? Weil die direkte Gefahr kaum spürbar ist. Trojaner, Würmer & Co. kommen quasi auf leisen Sohlen daher. Sei es über Mail-Angriffe, USB-Sticks, Zero-Day-Attacken (Ausnutzen von Sicherheitslücken vor dem Bereitstehen neuer Signaturen für Firewalls und Antiviren-Software) oder mithilfe von Backdoor Engineering durch korrumpierte Hard- und Software. Umstände, die betroffene User in der Regel nicht wahrnehmen, weil ein Großteil der Schadsoftware nicht bekannt oder nur schwer nachweisbar ist. Und fällt ein Eindringen – wie im Falle des Computervirus Stuxnet – auf, ist es meist zu spät. So konnte Stuxnet das Atomprogramm des Iran massiv beeinflussen und stören. Für Experten, wie Thomas Königshofen, ist die Qualität der Stuxnet-Schadsoftware ein Anzeichen dafür, dass hier mit großer Professionalität und langer Planung vorgegangen wurde.

Mittendrin statt nur dabei. Der Cyberkrieg ist längst Realität

Hinter diesen gezielten Angriffen stecken immer häufiger Staaten, die im Kampf um wirtschaftliche Macht und Interessen auf virtuelle Agenten setzen. Gegen diese Angriffsszenarien sind kaum Schutzmaßnahmen möglich. Nachrichtendienste wissen dies und bauen bei ihrer Spionagearbeit immer häufiger auf Trojaner und Virenprogramme. Sei es von außen eingeschleust oder mithilfe von Mitarbeitern.

Vor allem der „innere Feind“ sabotiert meist mit einfachen Tatwaffen, wie USB-Sticks, die organisationsweite IT-Infrastruktur, legt komplette Produktionen lahm oder hat beim Datendiebstahl leichtes Spiel. Für Frank Romeike, Moderator und Referent des Security Summit und Geschäftsführer der RiskNet GmbH, ist diese Entwicklung kein Wunder: „Die Sorglosigkeit mit der viele Unternehmen im Kampf gegen den Datenklau agieren macht vor allem eines klar. Es mangelt in vielen Fällen an Risikomanagement- und Awarenessprogrammen.“ Und darauf zielt der IT-Trainingsanbieter qSkills mit seinen Risikomanagement-Schulungen.
Oft können Mitarbeiter ungehindert an sensible Daten gelangen, diese mit der Handykamera fotografieren oder auf einen Datenträger kopieren und einfach entwenden. Und dieser Datendiebstahl kann Unternehmen teuer zu stehen kommen. Sei es in puncto eines Datenverlustes sensibler Unternehmensinformationen oder einem Imageschaden, der sich nicht in Zahlen beziffern lässt. „Meist werden Anti-Viren-Scanner und Firewalls installiert. Informationssicherheit beginnt jedoch bereits bei der morgendlichen Fahrt mit der S- oder U-Bahn zum Büro. Damit einher geht die mangelnde Einstellung zu Informationssicherheit und Risikomanagement vonseiten der Mitarbeiter“, so Frank Romeike. Im Klartext: Es fehlt eine gelebte Sicherheits- und Risikokultur.

Awareness schaffen heißt Mitarbeiter sensibilisieren

Um den möglichen Bedrohungen von Außen und Innen Herr zu werden, bedarf es klarer Spielregeln im Umgang mit wichtigen Unternehmensdaten. Hierzu gehört einerseits, Lieferanten genauer unter die Lupe zu nehmen. Will heißen bereits im Vorfeld die Vertrauenswürdigkeit von Hard- und Software zu prüfen. Dabei sollte die Frage im Mittelpunkt stehen, wer liefert überhaupt? Aus welchem Land stammen die IT-Produkte und kann ich als Unternehmen dem Zulieferer trauen? Hier ist Sorgfalt geboten, denn Spionagetechnologien werden gerne in IT-Lösungen versteckt – meist unauffindbar. Hinzu kommt, dass Unternehmen nicht alle Server, Notebooks oder Router auf links drehen und absichern können. Das übersteigt die Kapazitäten der meisten Unternehmen, sowohl in Bezug auf Zeit als auch den Kosten.

Ein wesentlicher Aspekt spielt beim modernen Datendiebstahl der Faktor Mensch. Seine Verhaltensweisen tragen meist zu Datenpannen bei. Über Social Engineering wird das persönliche Umfeld von Personen ausspioniert, um an Identitäten und Passwörter zu gelangen sowie in fremde Computersysteme einzudringen. Leicht wird es in diesem Zusammenhang dank Social-Media-Lösungen. Facebook, Twitter & Co. sind bei Unternehmen und Datendieben gleichermaßen beliebt. Während Organisationen über die neuen Kommunikationskanäle mehr und mehr Informationen verbreiten, nutzen Kriminelle und staatliche Stellen die Sorglosigkeit vieler Firmen gnadenlos aus.

Daten werden von potenziellen Opfern im Internet bereitgestellt und darüber lassen sich wiederum Verhaltensmuster von Firmenmitarbeitern ableiten, die von den Social Hackern bewusst aufgegriffen werden.
Dr. Werner Degenhardt von der Fakultät Psychologie und Pädagogik der Ludwig-Maximilian Universität München, verwies in seinem Vortrag im Rahmen des qSkills Security Summit auf die Lernfähigkeit von Mitarbeitern im Umgang mit Informationen und den dazugehörigen Verhaltensmustern.
Zum Erfolg werden solche Maßnahmen aber erst mit klaren Regeln und der Einsicht der Unternehmen, dass Mitarbeiter stärker in den Risikomanagement- und Awareness-Prozess integriert werden müssen. Oder wie Frank Romeike resümiert: „Egal wie viele Fälle von weißen Schwänen wir schon beobachtet haben, lässt das nicht den Schluss zu, dass alle Schwäne weiß sind. Unternehmen werden durch schwarze Schwäne ruiniert." Die Kunst des Risikomanagements liegt eben exakt darin, die potenziellen schwarzen Schwäne rechtzeitig zu erkennen.

Weitere Informationen zu qSkills unter: www.qskills.de

Für weitere Informationen:

qSkills GmbH & Co. KG
Birgit Jacobs
Telefon: +49 (0)911 80103-31
birgit.jacobs@qskills.de

Agenturkontakt:

Klartext Public Relations
Andreas Eicher
Telefon: +49 (0)69 976714-66
andreas.eicher@pr-klartext.de