die nicht in der Lage sind, die Ablaufkette moderner Datendiebstahl-Angriffe zu unterbrechen."

Der vollständige Report (in Englisch) kann nach einer Registrierung bei Websense heruntergeladen werden: *http://www.websense.com/content/2014-ponemon-report-part-2.aspx?cmpid=prnr7.17.14*

Systematischen Gefährdungsanalyse der IT

Obwohl ein Pflichtprogramm der Unternehmen, werden mögliche Gefährdungen der Informationstechnik nicht kontinuierlich ermittelt. Nach den Beobachtungen der mikado ag (*http://www.mikado.de/*) finden solche Risikoanalysen häufig nur punktuell oder ohne klare Systematik statt. Dabei ist eine präzise Kenntnis des Gefährdungspotenzials die Grundlage für ein bedarfsgerechtes Risikomanagement. Robert Hellwig, IT-Security-Analyst des Beratungshauses, hat Eckpunkte einer systematischen Risikoanalyse zusammengestellt:

Kenntnis der rechtlichen Anforderungen:
Die rechtlichen Bedingungen im Zusammenhang mit der IT sind heutzutage sehr vielfältig. Sie reichen vom Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) über das Bundesdatenschutzgesetz und die EU-Richtlinien zu den Datenschutzbedingungen bis zu Sarbanes-Oxley Act (SOX) und Basel III. Hinzu kommen branchenspezifische oder standesrechtliche Regelungen, die es zu beachten gilt. Auch Fragen der Vertragsregelungen wie etwa Vertraulichkeitsvereinbarungen mit Mitarbeitern oder Regelungen für den Datenschutz beim Outsourcing gehören dazu.

Kritikalitätsstufen der Unternehmensprozesse bewerten:
Nicht alle internen Abläufe erzeugen bei einem Ausfall ein hohes wirtschaftliches Sicherheitsrisiko, manche können bei gravierenden Störungen jedoch zu weitreichenden Konsequenzen führen. Dazu zählen beispielsweise viele marktnahe Prozesse, die bei einem Ausfall erhebliche Umsatzeinbußen oder Imageschäden bewirken können. Deshalb gilt es, sie nach Risikostufen wie „gering", „mittel" und „hochkritisch" einzuordnen. Auf Basis dieser Kategorisierung sollten sowohl die Risikovorsorge als auch die Maßnahmen für das Business Continuity Management in Problemfällen geplant werden.

Daten nach ihren Informationswerten kategorisieren:
In ähnlicher Weise wie die Kritikalitätsbewertung der Prozesse ist auch eine Analyse der Daten vorzunehmen. Ihr jeweiliger Informationswert und Verfügbarkeitsbedarf kann in einem Fall sehr elementar für das Unternehmen sein, in anderen Fällen sind die Folgen eines Datenverlustes relativ gering. Beispielsweise haben die Konstruktionspläne eines Produktherstellers einen hohen Informationswert, weil sie vermarktungsstarke Innovationen in sich bergen. Dagegen sind Informationen aus dem operativen Alltag einer Organisation häufig deutlich weniger sicherheitsrelevant.

Kritische IT-Infrastrukturkomponenten identifizieren:
Die erhebliche Abhängigkeit der Geschäftsprozesse von der IT verlangt eine hohe Verfügbarkeit der Anwendungen und Verarbeitungssysteme. Für ein Risikomanagement ist es deshalb wichtig zu wissen, welche Komponenten bei einem Ausfall den Geschäftsbetrieb oder wesentliche Teile der Organisation tiefgreifend beeinträchtigen. Deshalb gehört es zu den Grundlagen eines Risikomanagements, dass sie ebenfalls in die Kritikalitätsstufen „gering", „mittel" und „hochkritisch", bei Bedarf auch differenzierter, eingeteilt werden.

Eine Bedrohungs- und Schwachstellenanalyse vornehmen:
Für eine Vorbereitung auf mögliche Probleme bedarf es einer systematischen Betrachtung, welche Bedrohungs- und Katastrophen-Szenarien denkbar sind und welche Folgen damit verbunden wären. Zudem ist es erforderlich zu untersuchen, welche Schwachstellen bei den Infrastrukturkomponenten und Prozessen denkbar sind, die sich im Problemfall in weitreichender Weise negativ auswirken können. Sowohl die Eintrittswahrscheinlichkeit der Bedrohungs- und Katastrophen-Szenarien als auch die Wahrscheinlichkeit, dass dann die Schwachstellen davon betroffen sein können, müssen einschließlich der damit verbundenen Schadenshöhe kalkuliert werden.

Gefährdungsprofil in den Methoden des IT-Risikomanagements abbilden:
Durch die ermittelte Definition des konkreten Schutzbedarfs können gezielte Initiativen zur Risikominderung eingeleitet werden. Dies gehört zur Kernfunktion des IT-Risikomanagements als Königsdisziplin in der Informationssicherheit. Sie zielen darauf ab, mögliche Gefahren bereits in den Ansätzen zu erkennen und dort wo nötig vorbeugende Maßnahmen zu ergreifen.

G&D sichert die Zahlungsfunktion der digitalen Brieftasche von BASE

Mobilfunkkunden von BASE können ab sofort mithilfe der digitalen Brieftasche „BASE Wallet" im Smartphone kontaktlos an der Supermarktkasse, an der Tankstelle oder auch im Restaurant bezahlen - und das genauso sicher wie mit einer herkömmlichen Bank- bzw. Kreditkarte. Ermöglicht wird dieses hohe Sicherheitsniveau durch Giesecke & Devrient (G&D). Als Sicherheitspartner liefert G&D spezielle SIM-Karten mit hochsicherem Speicher, um die digitale Maestro-Karte zu speichern. Außerdem betreibt Giesecke & Devrient für E-Plus ein hochsicheres Rechenzentrum, um die Bezahlapplikation auf der SIM-Karte zu installieren, zu personalisieren und sie über ihren Lebenszyklus zu verwalten.

Besitzer NFC-fähiger Smartphones können mittlerweile in Deutschland an mehr als 35.000 Akzeptanzstellen kontaktlos bezahlen. Voraussetzung ist eine digitale Brieftasche mit eingerichteter Bezahlfunktion wie der digitalen Maestro-Karte. „Wir gehen davon aus, dass das kontaktlose Bezahlen mit Karte oder Smartphone in den nächsten Jahren zur Selbstverständlichkeit wird. Natürlich müssen alle Voraussetzungen für eine breite Akzeptanz in der Bevölkerung erfüllt sein. Kunden möchten flexibel und bequem bezahlen ohne auf die gewohnte Sicherheit zu verzichten", sagt Carsten Ahrens, Group Senior Vice President, Leiter der Division Telecommunication Industries bei G&D.

Und das ist bei der BASE Wallet der Fall. Die NFC-fähige SIM-Karte SkySIM CX fungiert als zentrales Sicherheitselement im Smartphone, um sensible Informationen zu speichern. Der Trusted Service Manager (TSM) im hochsicheren Rechenzentrum von G&D verwaltet zum einen den sicheren Bereich auf der SIM-Karte, zum an-