lekom-Konzerns, um Großkunden die volle Bandbreite an Sicherheitslösungen zu bieten.

Prävention, Erkennung und Reaktion als gleichberechtigte Aktionsfelder

Die beiden Unternehmen werden ihr gebündeltes Know-how über Cybersecurity und den Schutz von komplexen IT-Landschaften zunächst für die Beratung und Analyse von Großkunden-Systemen einsetzen. Das Leistungsspektrum reicht von der Analyse individueller Cyberrisiken für Unternehmen über die Hilfe beim Entwickeln von Cybersecurity-Strategien und -Architekturen bis hin zur Lieferung hochentwickelter Cybersecurity-Dienste. Sicherheitsfachleute entwickeln gemeinsam für Kunden ein operatives System, das die IT-Sicherheit des Unternehmens auf dem neuesten Stand steuert und das dynamisch auf Angriffe reagieren kann.

Ein solches Next Generation Security Operation Center (SOC) kombiniert dabei neueste Technologien mit dem Know-how der Cyberabwehr-Spezialisten von T-Systems und RSA. Prävention, Erkennung und Reaktion auf Sicherheitsvorfälle sind in diesem Vorgehensmodell gleichberechtigte Aktionsfelder.

Cyber Security Report 2013: Fast alle Unternehmen schon mal von Hackern attackiert

Die überwiegende Zahl von mittleren und großen Unternehmen in Deutschland berichtet von IT-Angriffen von außen. Nur 13 Prozent der Firmen sind dem Cyber Security Report 2013 zufolge noch nie aus dem Internet angegriffen worden. Ein Fünftel aller vom Institut für Demoskopie Allensbach befragten Unternehmen muss sich sogar täglich oder mehrmals in der Woche gegen Hackerangriffe wehren. Für die Studie haben die Marktforscher im Auftrag von T-Systems insgesamt 221 Führungskräfte aus großen sowie 293 Entscheider aus mittleren Unternehmen befragt.

Das Risiko steigt offenbar mit der Unternehmensgröße. Von den Unternehmen mit mehr als 1.000 Mitarbeitern meldete ein Drittel mehrere Angriffe pro Woche. Unter den kleineren Unternehmen mit bis zu 100 Mitarbeitern verzeichneten 16 Prozent häufige Attacken. Gleichwohl nimmt das Thema IT-Sicherheit der Umfrage nach für nahezu alle Unternehmen (92 Prozent) einen hohen Stellenwert ein. Das spiegelt sich auch in den Investitionen wider: 35 Prozent der Entscheider berichten über deutlich, 41 Prozent über etwas gestiegene Ausgaben in diesem Bereich.

Auch das Risikobewusstsein der Führungskräfte ist größer geworden: Während vor einem Jahr rund 42 Prozent der Großunternehmen das Schadensrisiko durch einen Hackerangriff als groß oder sehr groß einstuften, sind es aktuell 53 Prozent. Dennoch fühlt sich die Mehrheit der Unternehmen (56 Prozent) so gut wie möglich auf drohende Gefahren vorbereitet. Rund 40 Prozent besitzen sogar eine umfassende Strategie zum Umgang mit Cyber-Gefahren, 13 Prozent arbeiten daran. Allerdings setzen ebenfalls gut 40 Prozent nur auf Einzelmaßnahmen zum Sichern ihrer IT-Systeme und Firmendaten.

Sicherheitsbewusstsein von Mitarbeitern schärfen

Ein erhebliches Sicherheitsrisiko bergen nach Meinung der Führungskräfte die eigenen Mitarbeiter. 57 Prozent der Entscheider glauben, dass Angestellte, die leichtfertig mit Daten umgehen und Sicherheitsstandards nicht beachten, eine große oder sehr große Gefahr für das Unternehmen darstellen. Ebenfalls Bedrohungspotenzial hat nach Ansicht der Führungskräfte die zunehmende Nutzung mobiler Endgeräte, wie Smartphones und Tablet-PCs. 16 Prozent schätzen dies als sehr große, 34 Prozent als große Gefahr ein. Auf die Frage nach dem größten Handlungsbedarf beim Thema IT-Sicherheit nannten 23 Prozent der Führungskräfte die Schulung, Information und Sensibilisierung der Mitarbeiter. Trotz allem: 57 Prozent der Entscheider glauben, dass den meisten Mitarbeitern die Bedeutung der IT-Sicherheit durchaus bewusst ist.

Entscheider sehen Internet-Risiken kritischer als Bevölkerung Befragt wurden für den Cyber Security Report 2013 neben den Unternehmensvertretern auch 117 Abgeordnete. Dabei zeigte sich ein deutlicher Unterschied in der Risikoeinschätzung zwischen den Befragten aus Politik und Wirtschaft und der Bevölkerung. Den höchsten Risikowert mit jeweils 62 Prozent erhielten in der Befragung Datenbetrug im Internet und der Missbrauch von persönlichen Daten in sozialen Netzwerken. Unter der Bevölkerung erkannten 45 beziehungsweise 33 Prozent hier ein großes Risiko. Auch das Ausspähen von Telefon- und Internetdaten durch Geheimdienste beunruhigt deutsche Abgeordnete und Führungskräfte: Jeder vierte Befragte wertet die Spähaffäre als Risiko für unsere Gesellschaft. Vor einem Jahr äußerten sich nur 17 Prozent in diesem Sinne, also nicht einmal jeder Fünfte.

Rezensionen

Veranstaltungen

Britta Alexandra Mester

Tagungsbericht von der DSRI-Herbstakademie 2013, Berlin 11. – 14. September ‚Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter'

Die Herbstakademie 2013 der Deutschen Stiftung für Recht und Informatik (DSRI) fand in diesem Jahr vom 11. bis 14. September an der Humboldt-Universität zu Berlin unter dem Titel „Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter" statt. Die 14. Herbstakademie bot den über 280 Teilnehmerinnen und Teilnehmer auch in diesem Jahr wieder ein bemerkenswertes Angebot von aktuellen und praxisrelevanten Referaten und Diskussionen. Wegen der aktuellen Entwicklungen im Datenschutz nahmen Vorträge hierzu, neben weiteren beachtenswerten Beiträgen zu den Schwerpunktthemen: Internet- und Im-materialgüterrecht, Telekommunikations-, Straf- sowie Steuerrecht, einen wesentlichen Teil der Veranstaltung in Anspruch.

Bereits zu Beginn der Veranstaltung wurde unter der Moderation von Prof. Dr. Benedikt Buchner (Universität Bremen) durch Dr. Mirko Wieczorek ein Einblick in die sich aus der geplanten EU-Da-