IT-Security

»Wer seine Schwächen kennt, kann sich besser schützen«

Advanced Threats gefährden die Sicherheit unserer Unternehmen. ***Ein Gastkommentar*** von Vassil Barsakov, CEE & CIS Regional Sales Manager RSA, The Security Division of EMC.

Hacker-Attacken, die betriebliche und finanzielle Abläufe von Unternehmen stören, sensible Daten klauen oder die Infrastruktur sabotieren, mehren sich. Unter »Advanced Threats« versteht man Cyberattacken, die es vorrangig auf die Zugriffsrechte von Personen abgesehen haben, um an sensible Daten zu kommen. Sie sind innovativ und entschlossen und verwenden immer Custom-Malware, die nicht von Signaturen erkannt wird. Nur schwer können sich Unternehmen vor einem Cyberangriff dieser Art schützen. Mit dem Verlust sensibelster Daten geht zumeist auch ein Image- und Vertrauensverlust einher. Allein der durch einen Hackangriff entstandene Sachschaden reicht oft weit in den zweistelligen Millionenbereich hinein. Eine Schadensbegrenzung im Nachhinein erfordert eine sehr knappe Reaktionszeit und Expertenwissen, das oftmals intern nicht im notwendigen Maße zur Verfügung steht. Um ein solches Horrorszenario zu vermeiden und sich ausreichend gegen Angriffe von außen schützen zu können, ist es für Unternehmen ratsam, sich zu jedem Zeitpunkt mit möglichen Bedrohungen sowie der eigenen Sicherheitslage und den persönlichen Schwachstellen auseinanderzusetzen. Eine Studie des Carnegie Mellon CyLab im Auftrag von RSA hat gezeigt, dass Aufsichtsräte und Führungskräfte das Risikomanagement ernst nehmen. Dennoch gibt es deutliche Defizite beim Verständnis der Bewertung und Behandlung von IT-Sicherheitsrisiken im Zusammenhang mit dem Enterprise-Risk-Management. Konkret bedeutet dies, dass Vorstände noch nicht ausreichend verstehen, wie stark das Geschäft ihres Unternehmens von IT-Systemen und der sicheren Datenspeicherung abhängig ist.

Vassil Barsakov, RSA: »Wer seine Schwächen kennt, kann sich besser schützen.«

Smartphone **und Co gefährden**

Der zunehmende Einsatz von Smartphones und Tablets als Arbeitsmedien stellt Unternehmen vor neue Herausforderungen bei der IT-Sicherheit und beim Datenschutz. Manager und Unternehmer sehen im mobilen Computing ein gewaltiges Potenzial für die Steigerung des geschäftlichen Nutzens. Die Unterstützung einer größeren Gerätevielfalt bringt mehr Wahlfreiheit mit sich und ist, ebenso wie die Zulassung der Nutzung privater Geräte der Mitarbeiter, ein wachsender Trend, aber eben auch eine wachsende Bedrohung. Die Risiken können gravierend sein: Zu den wichtigsten Sicherheitsbedenken gehört der Verlust oder Diebstahl von Geräten und somit der Verlust vertraulicher Daten.

Risiken **minimieren**

Daher ist es unerlässlich, dass Sicherheitsexperten in Unternehmen eine führende Rolle übernehmen, um potenzielle Risiken und Gefahren zu minimieren. Ein erfolgreiches Risikomanagement erfordert bereichsübergreifende Zusammenarbeit, die Entwicklung von Richtlinien und Verfahren, die Berücksichtigung von Sicherheitsfragen beispielsweise bei der Planung der Mobilgerätestrategie und die Schulung der Anwender. Dazu muss eine Reihe geschäftlicher, betrieblicher und technischer Entscheidungen getroffen werden.

Abwehrmaßnahmen **entwickeln**

Jeder ist verwundbar, doch wer seine Schwächen kennt, kann sich besser schützen und gezielt Angriffe abwehren. Moderne Angreifer meinen es ernst und verfügen über Mittel, um häufig eingesetzte Schutzmaßnahmen zu umgehen. Durch die Auseinandersetzung mit den eigenen Schwächen und den Einsatz von IT-Sicherheitsexperten können sensible Daten besser geschützt und ein Angriff aus dem Netz leichter abgewehrt werden. Um die Sicherheitsstrategie eines Unternehmens erfolgreich auszurichten, können Big Data Scientists die IT-Experten unterstützen. Unternehmen müssen sich aktuelle Daten zu Bedrohungen verschaffen und diese mithilfe von Big Data Analytics auswerten. Ein solches System ist imstande, in Echtzeit umfassende Netzwerk- und Log-Daten sowie Warnsignale aus bestehenden Sicherheitssystemen wie Firewalls mit Threat-Intelligence Feeds zu korrelieren, um handlungsorientierte Informationen zu erhalten. Diese Daten sollten zu anderen relevanten Fakten in Beziehung gesetzt werden. Wertvoll werden die Daten dann, wenn sich daraus Abwehrmaßnahmen ableiten lassen, die ein Unternehmen dabei unterstützen, gegen laufende Advanced Threats vorzugehen. ❐

Foto: RSA/EMC