Themen 2010: Automatische Hackerangriffe, Cloud Computing, Kosten für Sicherheitsvorschriften, neue Gefahren, Minimierung der Angriffsfläche

SANTA CLARA, Kalifornien – 4. März 2010
Sentrigo, Inc., der Wegbereiter in Sachen Datenbankschutz, gibt einen Ausblick auf das, was in 2010 zu diesem Thema zu erwarten ist.

Die ständigen Auseinandersetzungen zwischen Hackern und Datenschützern im letzten Jahr hatten zur Folge, dass beide Seiten ihre Techniken verbessert haben und dies auch weiterhin tun. Je besser man voraussagen kann, was der Gegner vorhat, desto besser ist das eigene Team darauf vorbereitet, Angriffe abzuwehren. Wir stellen Ihnen im Folgenden einige Thematiken vor, die sich nach unserer Meinung am schnellsten ändern und unter Umständen Ihren gesamten Plan zur Datensicherheit beeinflussen könnten:

Hacker haben Zugang zu besseren Tools

Im vergangenen Jahr setzten Kriminelle in aller Welt verstärkt Open Source Software zu immer raffinierteren Zwecken ein und im Jahr 2010 werden die Hacker diese Tools noch gewiefter anwenden. Dadurch werden diese Tools immer leistungsfähiger. Updates und neue Funktionen erlauben es auch ungeübteren Hackern, sich Zutritt zu Datenbanken mittels ausgefeilter Technik zu verschaffen. Dies hat völlig willkürliche Zufallsattacken zur Folge, die nicht länger auf ein bestimmtes Unternehmen abzielen, sondern nach spezifischen Sicherheitslücken suchen, wo auch immer sich diese befinden. Die vierteljährlich von Oracle herausgegebenen CPU (Critical Patch Updates) oder die vielen von Microsoft publizierten „Dienstags“-Patches geben immer wieder neue Sicherheitslücken bekannt. Prompt werden diese in die Hacker-Toolkits eingebaut und haben sofortige Angriffe auf eben jene Sicherheitslücken zur Folge.

Sicherheitslösungen für Cloud Computing in Sicht!

Viele Unternehmen zögern aus Sicherheitsgründen, Cloud Computing für Anwendungen mit sensiblen Daten einzusetzen. Bestehende Sicherheitsvorschriften verlangen nachweisbare Beweise darüber, dass Kreditkartendaten und personenbezogene Daten (PII) vorschriftsgemäß verarbeitet werden. Aber auf welche Art kann man Daten schützen, wenn man nicht einmal weiß, auf welchem Server sie abgelegt sind? Häufige Datenbewegungen führen dazu, dass die Daten kopiert werden, ohne dass dies bemerkt wird. Auch ändern sich die Anwendungen, die auf die Daten zugreifen, ständig und sind somit ebenfalls Grund für mögliche Sicherheitslücken.

Demnächst sind neue Sicherheitslösungen verfügbar, die Probleme bei der Datensicherung im Cloud Computing beheben sollen. Mit Methoden, die Datenprüfungen auf darunterliegenden Datenbanken durchführen sowie Policies (Richtlinien) und Protokolle zentral verwalten, können Daten auch in sehr dynamischen Umgebungen gesichert werden.

Wirtschaftlichkeit trotz Zwang zur Einhaltung kostenintensiver Vorschriften

Unternehmen wissen, dass sie Richtlinien ihres jeweiligen Industriestandards befolgen müssen. Die gegenwärtige wirtschaftliche Lage erfordert aber, alle Kosten eingehend auf den Prüfstand zu stellen. Die meisten investieren deshalb nur in Lösungen bis zu einem Sicherheitsgrad, der dem absoluten Minimum der Vorschriften entspricht. Die Entscheidung darüber, welche Technik eingesetzt werden soll, orientiert sich meist daran, welches Produkt den passenden Schutz bei gleichzeitig möglichst geringen Gesamtkosten beim Kauf bietet. Folgende Fragen stehen im Vordergrund: wie problemlose ist die Installation, wie hoch sind die Kosten, wie schnell erfolgt die Umsetzung.

Im Zuge der wirtschaftlichen Erholung beginnen allerdings die Marktführer, den Sicherheitsaspekt höher anzusetzen und denken über verbesserten Schutz nach.

Die neue Gefahr: Externe Angriffe aus dem Netzwerk heraus

Bei Angriffen auf ein Netzwerk denken wir meist an solche von außerhalb der Netzwerkumgebung oder an Internetbenutzer, die ihre Zugangsberechtigungen missbrauchen. Diese klare Abgrenzung wird im Jahr 2010 verschwimmen, denn die Zahl der Angriffsmöglichkeiten nimmt ständig zu:

- Das organisierte Verbrechen spioniert bestimmte Unternehmen durch das Einschleusen von sogenannten „Schläfern“ aus, die das Unternehmen getarnt als Mitarbeiter oder Vertragspartner mit der Absicht infiltrieren, sich Zugang zu sensiblen Daten zu verschaffen;
- Ein einfaches Aufrufen der Website kann schon ein Herunterladen neuer Arten von Schad-Software zur Folge haben, die selbstständig innerhalb des Netzwerkes angreift und die Firewall nicht mehr zu durchdringen braucht;
- Anhaltende und drohende Arbeitslosigkeit macht Betroffene empfänglich für Bestechungsgelder und Erpressung. Immer häufiger kommt es daher vor, dass Insider Außenstehenden Zugang zu vertraulichen Daten beschaffen.

Sich gegen diese Art des Missbrauchs zu wehren, erfordert Lösungen, die die Daten unabhängig von der Herkunft des Angriffes schützen. Daher sollte es ein wichtiger Bestandteil der Datensicherheitsstrategien jedes Unternehmens sein, die Schutzmaßnahmen über die Firewall oder die Netzwerküberwachung hinweg auszudehnen.

Minimierung der Angriffsfläche verringert die Anfälligkeit

Ebenso wie die Policy zur Reduzierung von Email Speicherung den Gefährdungsgrad bei E-Discovery einschränkte, werden Unternehmen dazu übergehen, umgehend und in großem Umfang sensible Daten nach der Verarbeitung sofort aus dem Netz zu nehmen. „Muss man denn unter allen Umständen die Aufzeichnungen über Unterrichtsgebühren eines jeden Schülers, Steuererklärungen und Bankkontodaten aufbewahren, nachdem die betreffenden Schüler den Schulabschluss gemacht haben? Oder wenn bei einer Kreditkartenüberweisung das Dialogfenster für den Transfervorgang geschlossen wurde, braucht man dann noch die Daten des Kreditkartenbesitzers?“ fragt Slavik Markovich,

Technischer Direktor und Mitbegründer von Sentrigo, zu Recht. Jede Situation stellt sich anders dar und sollte mit einer genauen Abwägung des zugrundeliegenden Geschäftsvorganges betrachtet werden – aber bei Fällen, in denen ältere, sensible Daten einfach gelöscht werden können, müssen auch infolgedessen weniger Daten insgesamt geschützt werden.

Über Sentrigo

Sentrigo, Inc. ist ein anerkannter Spezialist für Datenbanksicherheit. Sentrigos Sicherheitslösung Hedgehog bietet ein weit reichendes Monitoring aller Datenbankaktivitäten und die Absicherung der Datenbanken in Real-Time. Die Software-basierte Lösung ist weltweit bei 2000 Firmen im Einsatz, um unternehmenskritische Daten gegen Missbrauch durch Insider aber auch gegen Angriffe von außen zu schützen. Unternehmen aus allen Industriesegmenten nutzen Hedgehog zur schnelleren Unterstützung und Umsetzung bei der Einführung und Überwachung von Regularien wie PCI DSS, Sarbanes-Oxley und HIPAA. Sentrigo wurde für die technologische Innovation von verschiedenen Publikationen, wie Network World und SC Magazine ausgezeichnet. Nähere Informationen zu Hedgehog finden Sie unter www.sentrigo.com.

Pressekontakt USA:
Rachel Kaseroff - MarComm PR - +1 (415) 824-1110
Email: Rachel@marcommpr.com

Pressekontakt in Deutschland:
Beatrice Brenner -MBS Marketingberatung
Ostring 27 - 63820 Elsenfeld
Email: bb@mbs-brenner.com
Tel : +49 60 22 / 64 91 87, Fax: +49 60 22 / 64 91 83,
mobil +49 175 5230 788