Kommentar von Clavister: Hat PRISM das Vertrauen in die IT erschüttert?

Kommentar von Clavister: Hat PRISM das Vertrauen in die IT erschüttert?

Im IT- und Kommunikationsmarkt ist es aktuell schwierig, der Offenlegung zu entfliehen, die mittlerweile als "rechtmäßige Überwachung" bekannt wurde. Dies ist ein bekanntes Konzept für Personen, die in der Security-Industrie tätig sind, aber auch für Mitglieder der Öffentlichkeit: Normalerweise wird für eine Überwachung ein Gerichtsbeschluss benötigt, bevor sie in Kooperation mit dem ISP (Internet ServMice Provider), dem Telekommunikationsbetreiber oder dem Netzwerkanbieter ausgeführt wird. Dies ist ein gut dokumentierter, klar nachzuverfolgender Prozess auf einer gesetzlichen Grundlage und ohne Überraschungen.
Jedoch hat die Enthüllung des NSA-Überwachungsprojektes PRISM, das Zugang im industriellen Maßstab zu Daten- und Voice-Traffic, gespeicherten Informationen, Dateiübertragungen und Aktivitäten in sozialen Netzwerken sowohl von Privatpersonen als auch Unternehmen ohne deren Wissen oder Erlaubnis, einen Aufschrei der Massen ausgelöst.
Es ist schlimm genug, dass Cyberkriminelle seit Jahren illegal auf Daten und geistiges Eigentum zugreifen und dies zu ihren eigenen Zwecken verwenden - aber es ist noch schlimmer herauszufinden, dass Regierungsbehörden dasselbe getan haben könnten. Und während Regierungsbeamte schleunigst die Unternehmen und die Öffentlichkeit informieren, dass PRISM bei ihnen nicht eingesetzt wurde, sowie Sicherheitsklauseln existieren, die sicherstellen, dass ihre Daten und Speicher nicht kompromittiert wurden, trägt das nur wenig dazu bei, irgendjemanden zu beruhigen.
Das "vertraute Netzwerk" untergraben
Natürlich gehen seit einiger Zeit Spekulationen um, dass die Geheimdienste der mächtigsten Länder dazu imstande waren, Einzelpersonen rechtswidrig zu monitoren sowie Informationen mittels detaillierter Kenntnisse von Netzwerk- und Security-Lösungen sowie Software zu sammeln. Jetzt, da diese Vermutungen durch die Neuigkeiten über PRISM bestätigt zu sein scheinen, wirft dies eine wichtige Frage auf: Kann Equipment und Software aus Ländern, die in diese Informationssammlung verwickelt sind, wirklich komplett vertraut und sich in puncto Security auf sie verlassen werden?
Aktuelle Entwicklungen, die multinationale Konzerne berühren, die den größten Teil an Netzwerkequipment, Kommunikationsapplikationen und Suchmaschinen bereitstellen, die die Infrastruktur des Internets und anderer globaler Netzwerke formen, lassen potenzielle Bedrohungen der Vertraulichkeit erkennen. Bedrohungen sowohl für die persönliche Privatsphäre als auch für Enterprise Intelligence und die nationale Sicherheit.
Fakt ist, dass die Mehrheit aller Internetsuchen eine einzige Suchmaschine verwenden, ein beträchtlicher Teil der Smartphones kommt von einem Anbieter und der Großteil der Betriebssysteme und Cloud-E-Mail-Server stammt von nur einer Quelle. Jede dieser Organisationen könnte ihrer jeweiligen Regierung mit Informationssammlungen bezogen auf nationale Sicherheit oder vielleicht auch für wirtschaftliche Vorteile unterstützen.
Vertrauen Sie mir - und meinen 800.000 Kollegen
Daraus ergeben sich weitere Fragen. Kann diesen Anbieter hinsichtlich privater Informationen oder sensiblem geistigem Eigentum vertraut werden? Könnten vertrauliches Business Intelligence-Daten und geistiges Eigentum heimlich an sich genommen und für wirtschaftliche Gewinne genutzt werden? Diese Aktivitäten müssen nicht von einer Regierungsstelle unterstützt werden: In den USA besitzen mehr als 800.000 Personen höchste Sicherheitsfreigaben. Das sind ungefähr so viele Menschen, wie Stockholm Einwohner hat. Kann jedem Einzelnen dieser 800.000 Menschen uneingeschränkt vertraut werden? Zur Erinnerung: Wir wissen jetzt von PRISM auf Grund der Handlungen einer Einzelperson, die Zugang zu Top-Secret-Materialien hatte.
Cloud-basierte Anwendungen, bereitgestellt von Facebook, Google, Skype, Yahoo und anderen, werden verbreitet von Unternehmen genutzt, um Kunden anzulocken und Beziehungen zu ihnen aufzubauen. Banken beispielsweise können mit Kunden interagieren, indem sie Applikationen auf Social-Network-Seiten nutzen. Selbst wenn während einer Besprechung keine vertraulichen Informationen ausgetauscht werden, könnte sich dennoch über die Anwendung ein Weg in die Serverfarm der Bank öffnen, um geschützte Informationen abzufragen.
Mögliche Hintertüren in Netzwerkequipment wie Security Gateways und Firewalls müssen ebenso berücksichtigt werden. Falls solche "Backdoors" existieren, könnten sie einem externen Dritten einen unauffindbaren Weg einräumen, um den Traffic-Fluss zu beeinflussen. Eine Methode, sich eine Hintertür in Netzwerk zunutze zu machen, nennt sich "Dynamic Port Knocking". Es lässt sich nicht ermitteln und hinterlässt keine Spuren, aber kann einem Externen totale Kontrolle verleihen und ihm erlauben, internen Traffic abzuhören.
Während sich West und Ost gegenseitige Anschuldigungen an den Kopf werfen, wer in welchem Ausmaß auf welche Informationen zugegriffen hat und die in PRISM genannten Hersteller Dementi abgeben - Wo bleiben dabei die Unternehmen, die ernsthafte Fragen zu der Integrität und Vertrauenswürdigkeit ihrer Netzwerk- und Security-Lösungen haben?
Ich denke, dass Unternehmen damit beginnen werden, zu bewerten, wie hoch ihr Risiko ist, der behördlich geduldeten Schnüffelei ausgesetzt zu sein. Sie werden den Gebrauch von und das Vertrauen in Lösungen der etablierten "großen Namen" sowohl aus dem Westen als auch dem Osten überdenken und Alternativen evaluieren, die nicht mit diesem Vertrauensverlust behaftet sind. Wie ein altes Sprichwort besagt: Vertrauen ist wie ein Spiegel; es lässt sich reparieren, wenn es gebrochen wurde, aber man sieht noch immer die Risse.
Mehr Informationen stehen unter www.clavister.com bereit.
Von John Vestberg, CEO Clavister

Kurzporträt Clavister:
Gegründet im Jahr 1997, ist Clavister ein führender Mobile- und Network Security-Provider. Die preisgekrönten Lösungen basieren auf Einfachheit, gutem Design und sehr guter Performance, um sicherzustellen, dass Cloud-Service-Anbieter, große Unternehmen und Telekommunikationsbetreiber den bestmöglichen Schutz gegen die digitalen Bedrohungen von heute und morgen erhalten. Alle Produkte sind in einem skandinavischen Design entworfen, gekoppelt mit schwedischer Technologie. Clavister hält außerdem einen Weltrekord für den schnellsten Firewall-Durchsatz. Weitere Informationen erhalten Sie unter www.clavister.com .

Weitere Informationen:
Clavister Deutschland
Bülowstraße 20
D-22763 Hamburg
Ansprechpartner:
Thomas Gross
Tel.: +49 (40) 41 12 59 - 0
Fax: +49 (40) 41 12 59 19
E-Mail: Sales-DE@clavister.com
 www.clavister.de
PR-Agentur:
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
Ansprechpartner:
Fabian Sprengel
Tel.: +49 (26 61) 91 26 0 - 0
Fax: +49 (26 61) 91 26 029
E-Mail: fs@sprengel-pr. com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=537628" width="1" height="1">

Pressekontakt

Clavister

22763 Hamburg

Sales-DE@clavister.com

Firmenkontakt

Clavister

22763 Hamburg

Sales-DE@clavister.com

Clavister ist ein führender Hersteller von hoch performanten IT-/IP-Security-Lösungen. Die mehrfach international ausgezeichneten Produkte basieren auf der einzigartigen Clavister-Technologie. Diese beinhaltet Carrier Class Firewalls, Security Gateway- sowie VPN-Lösungen, die weltweit bereits von tausenden zufriedenen Kunden eingesetzt werden. Der Anspruch von Clavister liegt darin, seinen Kunden komplette Security-Lösungen anzubieten, die über ein herausragendes Preis-Leistungs-Verhältnis verfügen. Clavister wurde 1997 in Schweden gegründet, wo sich auch das Headquarter (Örnsköldsvik) sowie das Forschungs- und Entwicklungszentrum befinden. Die Produkte werden über eigene Niederlassungen in Europa und Asien sowie über ein internationales Netz von Distributions- und Reseller-Partnern vertrieben. In Deutschland sind die Produkte über die sysob IT-Distribution (www.sysob.de) und Tworex Trade (www.tworex-trade.de) erhältlich. Die deutsche Clavister-Niederlassung hat ihren Sitz in Hamburg. Weitere Informationen zu Clavister und den Produkten erhalten Sie unter: www.clavister.de.