Hacking-Angriff auf Gemalto: ein unbehagliches Déjà -vu-Gefühl

Hacking-Angriff auf Gemalto: ein unbehagliches Déjà -vu-Gefühl

Kommentar von Jim Carlsson, CEO bei Clavister
Kürzlich wurde bekannt, dass der US-Geheimdienst NSA und sein britisches Pendant GCHQ das Digital Security-Unternehmen Gemalto gehackt und dabei Millionen Verschlüsselungscodes von SIM-Karten gestohlen haben. Es soll der IT-Security- und Kommunikationsindustrie verziehen sein, wenn sie dabei ein starkes Déjà -vu-Gefühl überkommt. Weniger als zwei Jahre zuvor, seit den ersten Enthüllungen von Edward Snowden, kommen die Neuigkeiten vielleicht nicht überraschend, aber wieder einmal fragen sich Firmen weltweit, wer hinter ihren Daten her ist.
Während "Lawful Interception", die rechtmäßige Überwachung, als gut dokumentierter Prozess auf legaler Basis ohne Überraschungen stets akzeptiert wurde, führte die Aufdeckung staatlich unterstützter Hacking-Angriffe und Überwachungsmaßnahmen international zu massiven Verurteilungen. Nach den ersten Snowden-Enthüllungen überschlugen sich Regierungsbeamte förmlich, Unternehmen und der Öffentlichkeit mitzuteilen, dass PRISM, das NSA-Überwachungsprojekt für Daten- und Sprachaustausch, nicht bei ihnen eingesetzt worden sei. Zudem wurde gebetsmühlenartig erklärt, dass zahlreiche Sicherheitsvorkehrungen bestünden, um den Diebstahl von Daten und Aufzeichnungen zu verhindern. Angesichts des Gemalto-Hacks und jüngsten Berichten darüber, dass die CIA unbedingt die Verschlüsselung von Apple durchbrechen wolle, ist allerdings nachvollziehbar, dass Unternehmen wenig überzeugt davon sind, nicht selbst in der Schusslinie zu stehen.
Gemeinschaftssinn eröffnet Hintertüren
Nicht nur staatlich geförderte Attacken stellen für IT-Abteilungen Risiken dar; auch Backdoors in Netzwerk-Equipment wie Security Gateways und Firewalls sind akute Gefahrenstellen. Auch wenn sie sich vom Wesen her stark unterscheiden, haben die Heartbleed- und Shellshock-Angriffe verdeutlicht, dass selbst die robustesten Security-Lösungen durch Schwachstellen in der Codierung unterwandert werden können. Beide nutzten einfache Coding-Fehler aus, und das Hauptproblem war nicht der Fehler an sich, sondern eher die Annahmen tausender Menschen weltweit, was die Integrität und Sicherheit von Open Source Coding angeht.
Dem Unbekannten gegenüberstehen
Unternehmen sehen sich der großen Herausforderung gegenüber, zu erkennen, wer sie angreift und warum. Wie Gemalto bewiesen hat, ist es fast unmöglich, festzustellen, ob man Ziel von Überwachungsorganisationen ist. Und noch gibt es auch keine internationale Internet Security Task Force, die aktiv nach Coding-Schwachstellen sucht und sie nach Entdeckung schließt. Klar ist, dass es für Organisationen immer schwieriger wird, herauszufinden, wem und welchen Lösungen sie vertrauen können. Jede Organisation innerhalb der Wertschöpfungskette könnte zu jeder Zeit dazu aufgefordert werden, einer Landesregierung Informationen zur Verfügung zu stellen und damit auch Schlüssel zu Daten auszuhändigen. Zur gleichen Zeit könnte ein Unternehmen einem Cyberkriminellen ausgeliefert sein, der kurz davor ist, aufzudecken, dass das Kernsystem, auf das zum Schutz des Netzwerks vertraut wird, von einem einfachen Coding-Fehler betroffen ist.
Seit PRISM ist sicher anzunehmen, dass die Geheimdienste der Supermächte die Fähigkeit haben, scheinbar ungehindert Unternehmen und Privatpersonen zu überwachen, um Informationen zu sammeln. Ist es wirklich klug, Firmen Zugang zu unternehmenseigenen Richtlinien und Daten zu gewähren, in deren Herkunftsländern die Regierungsbehörden jederzeit und ohne ordentliches Gerichtsverfahren ebenfalls darauf zugreifen könnten?
Open Source-Codierungen wiederholt testen
Zudem sollten Firmen sicherstellen, dass alle ihre Lösungen unter strengen Vorgaben entwickelt, getestet und nochmals geprüft werden, um sicherzustellen, dass alle Schwachstellen eliminiert wurden. Natürlich wissen Hacker um das blinde Vertrauen von Unternehmen auf eine Menge ungetestete Codierungen in Websites, Apps, Security-Lösungen etc. Und dies eröffnet den Kriminellen wiederum Unmengen Angriffsgelegenheiten. Wenn Unternehmen weiterhin die Vorteile von Open Source nutzen und umsetzen möchten, ist es offensichtlich, dass Open Source-Codierungen wiederholt getestet werden müssen, um potenzielle Schwachpunkte zu reduzieren, bevor sie eingerichtet werden, unter der Annahme, sie seien sicher.
Ob PRISM, Gemalto-Hack, Heartbleed und Shellshock: Unternehmen vertrauen auf die Transparenz der Regierungen und die Robustheit von Open Source Codings, ohne zu prüfen, ob ihr Vertrauen auch gerechtfertigt oder verdient ist. Und wenn Organisationen immer wiederkehrende Déjà -vus verhindern wollen, ist unverdientes Vertrauen ein Luxus, den sie sich einfach nicht länger leisten können.
Hochauflösendes Bildmaterial kann unter clavister@sprengel-pr.com angefordert werden.
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 Niederlassung Deutschland
Paul-Dessau-Straße 8
D-22761 Hamburg
Ansprechpartner:
Thomas Gross
Tel.: +49 (40) 41 12 59 - 0
Fax: +49 (40) 41 12 59 19
E-Mail: Sales-DE@clavister.com
URL: 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_=590921" width="1" height="1">

Pressekontakt

Clavister

22763 Hamburg

clavister.de
Sales-DE@clavister.com

Firmenkontakt

Clavister

22763 Hamburg

clavister.de
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.