Security-Lücke "Heartbleed: So lassen Sie Ihre IT nicht ausbluten

Security-Lücke "Heartbleed": So lassen Sie Ihre IT nicht ausbluten

Kommentar von David Sandin, Produktmanager bei Clavister
Der Herzschmerz ist momentan in aller Munde, aber nicht aus zwischenmenschlicher, sondern aus IT-technischer Sicht: Kürzlich wurde "Heartbleed" entdeckt, eine Schwachstelle im OpenSSL-Security-System. Durch diese Sicherheitslücke können private Schlüssel des Serverzertifikats, Benutzernamen und Passwörter ausspioniert werden, und das schon seit rund zwei Jahren. Tatsächlich trifft sie das Herz des Internets, denn zahlreiche internationale Webseiten nutzen die Verschlüsselungssoftware. Clavister-Lösungen sind nicht berührt, da sie kein OpenSSL einsetzen. Was Sie als Betroffener jetzt tun können.
Die Lücke besteht in den OpenSSL-Versionen 1.0.1 bis einschließlich 1.0.1f sowie 1.0.2-beta bis einschließlich 1.0.2-beta1. Daher empfiehlt es sich für Unternehmen, entweder auf die letzte gefixte Version 1.01g zu aktualisieren oder OpenSSL ohne die betroffene "Heartbeat"-Erweiterung des TLS-Protokolls neu aufzusetzen. Möglicherweise wurden zwischenzeitlich die Zertifikate des Webservers kompromittiert oder sogar gestohlen. Aus diesem Grund ist es ratsam, die zuständige Zertifikatsbehörde zu kontaktieren, um einen Ersatz zu erhalten. Zusätzlich sollten Firmen Enduser-Passwörter zurücksetzen, die im Speicher eines attackierten Servers sichtbar gewesen sein könnten.
Erhöhtes Phishing-Risiko
Private Nutzer finden im Artikel des IT-Blogs Mashable eine Zusammenfassung aller Websites und Services, die wahrscheinlich betroffen sind. Außerdem erhalten sie Hilfestellung, ob sie ihre Passwörter ändern müssen. Darüber hinaus sollten sie in ihrem E-Mail-Postfach Vorsicht walten lassen: Es ist mit einem erhöhten Aufkommen an Phishing-Nachrichten zu rechnen, die die Angst vor der Heartbeat-Lücke ausnutzen. Beispielsweise könnte dazu aufgefordert werden, Kennwörter unter einem angegebenen Link zu ändern. Diese Links können allerdings zu bösartigen Websites führen. Passwörter sollten deshalb nur auf der offiziellen Seite des Betreibers direkt geändert werden.
"Annehmen" ist nicht gleich "wissen"
Der Kern dieser Sicherheitslücke ist ein einfacher Codierungsfehler, der jedem Entwickler unterlaufen kann. Aber für mich haben erst die Annahmen der Nutzer dazu geführt, dass Heartbleed international Schlagzeilen machte:
Annahme Nr. 1: Jemand wird den Code gegengeprüft und auf Sicherheit getestet haben, bevor er der OpenSSL Software Repository hinzugefügt wurde.
Annahme Nr. 2: Da in der Open Source-Entwicklung eine Gemeinschaft von Programmierern ohne kommerzielle Zwänge zusammenarbeitet, wird die Software vermutlich weniger Bugs aufweisen.
Annahme Nr. 3: Weil OpenSSL bei Zehntausenden Websites weltweit eingesetzt wird, darunter einige der größten Online-Marken, sowie von Herstellern in zahlreiche Security-Lösungen integriert wird, ist es wahrscheinlich vollständig getestet, stabil und sicher.
Im Zuge von Heartbleed haben sich diese Annahmen als falsch erwiesen. Eines möchte ich unmissverständlich klarstellen: Weder kritisiere noch befinde ich Open Source Software-Entwicklung für schuldig, ebenso kritisiere ich niemanden, der an der Entwicklung, dem Einsatz oder der Nutzung von OpenSSL beteiligt war. Fehler und Schwachstellen passieren, das kommt auch bei der international populärsten, kommerziellen Software vor, wie der monatliche "Patch Tuesday" beweist.
Blindes Vertrauen
Der blinde Ansturm auf den Einsatz von OpenSSL - weil es "jeder" nutzt und es durch den Open-Source-Ansatz kostenfrei ist - spielte eine wesentliche Rolle in Bezug auf das Ausmaß und die Schwere der Heartbleed-Lücke. Es scheint, als ob Hersteller sich nicht darum bemüht haben, den Code zu prüfen, bevor sie ihn in ihre Lösungen eingebaut haben. Dadurch haben viele End-User-Unternehmen Security-Produkte implementiert, die betroffene Code-Versionen einsetzen, um Anwendungen und Web-Services zu schützen, die ebenfalls OpenSSL nutzen und damit dieselbe Schwachstelle haben. Dies gibt Cyber-Kriminellen die Möglichkeit, die Sicherheitslücke gleich doppelt auszunutzen.
Überflüssige Codezeilen?
Aktuell arbeitet eine Open-Source-Software-Gruppe an einer vereinfachten, bereinigten Version von OpenSSL. Sie hat bereits fast 250.000 Codezeilen sowie unbenötigten Content entfernt. Wenn so viele Zeilen gelöscht werden konnten, wie viele sind dann komplett irrelevant für die Nutzung auf einem Network Security Gateway oder einer Firewall? Kommen im Unternehmen Firewall-Lösungen von Clavister zum Einsatz, kann sich der Puls des IT-Teams wieder beruhigen. Denn der schwedische Hersteller setzt weder OpenSSL noch andere Open Source-Produkte ein, um nicht ungewollt Schwachstellen, Backdoors und Bugs von Drittanbietern zu importieren.
Vertrauen plus Technik
Sicherheitslösungen müssen penibel entwickelt und mehrmals getestet werden, um zu gewährleisten, dass jegliche Schwachstellen eliminiert worden sind. Sie sollten nicht auf einem Code "von der Stange" beruhen oder einen solchen einsetzen, dessen Sicherheit nicht verifiziert ist - unabhängig davon, wie reizvoll dies sein mag, um die Entwicklung neuer Produkte zu beschleunigen. Security bedeutet Vertrauen, basierend auf einer soliden technischen Grundlage. Und das trifft auf Konsumenten, wichtige Websites und IT-Security-Hersteller zu. Das Internet hält schon genug Bedrohungen und Schwachstellen bereit, wir müssen es nicht noch gefährlicher machen, indem wir besorgniserregende Annahmen treffen.
Weitere Informationen hat Clavister in einem PDF zum Download unter http://documents.sysob.com/clavister/clavister-info-heartbleed-comment-en.pdf bereitgestellt.
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
 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_=564771" 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.