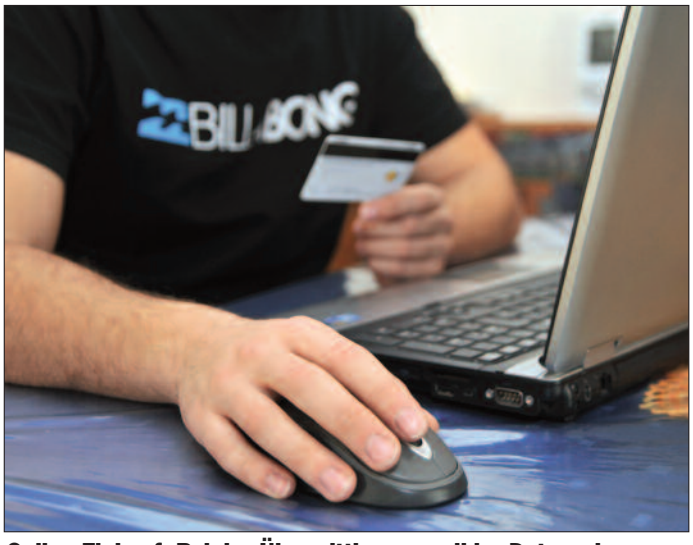
Verschlüsseln schützt

Experten des Computer-Emergency-Response-Teams gaben am 6. August 2014 in Wien einen Überblick über die IT-Sicherheitslage betreffend die Sicherheitslücke „Heartbleed“ in Österreich.

IT-Sicherheitsexperten entdeckten im April 2014 eine schwerwiegende Sicherheitslücke in der zum Schutz von Netzwerkverbindungen eingesetzten Internet-Sicherheitssoftware *OpenSSL* – genannt *Heartbleed*. „Bei der Heartbleed-Lücke handelt es sich um einen simplen Programmierfehler in der Verschlüsselungssoftware OpenSSL“, sagt Otmar Lendl, Teamleiter im *Computer Emergency Response Team (CERT.at)*. „Heartbleed“ sei deshalb so gravierend gewesen, weil weltweit der Zugriff auf Server-Programme mittels *OpenSSL* abgesichert wird. Durch die Lücke sei es Angreifern möglich gewesen, geheime Schlüssel, Nutzernamen, Passwörter, E-Mails und Dokumente zu stehlen. Hunderttausende Server waren angreifbar, auch Systeme in Österreich waren von dieser Sicherheitslücke betroffen.



Online-Einkauf: Bei der Übermittlung sensibler Daten wie Kontonummern und Passwörter sollte die Verbindung verschlüsselt erfolgen.

„Heartbleed hat der Welt vor Augen geführt, dass Software – egal ob open oder closed Source – in den seltensten Fällen fehlerfrei ist“, betont Lendl. Viele Sicherheitsvorfälle würden nach einem ähnlichen Muster ablaufen. Das Besondere bei *Heartbleed* sei nicht die Sicherheitslücke an sich, sondern die große Anzahl der betroffenen IT-Systeme und das damit einhergehende Schadpotenzial.

„Die Unterwanderung des bislang als sicher geltenden Internetprotokolls SSL hat dazu geführt, dass sich *Heartbleed* binnen kürzester Zeit nach dessen Bekanntwerden zu einem der weltweit größten IT-Sicherheitsvorfälle entwickelt hat“, erklärt Lendl.

Information. Aufgabe der Experten von *CERT.at* war es, herauszufinden, welche Web- und Mail-Server auf *Heartbleed* anfällig sind, und die betroffenen Betreiber zu informieren. Bis 6. August 2014 versendete das *CERT*-Team 4.366 Meldungen an 694 Internet-Service-Provider. Weiters überprüften die IT-Spezialisten rund 1,2 Millionen Domains der .at-Zone hinsichtlich ihrer *Heartbleed*-Anfälligkeit. Unter den Servern, die SSL-Verschlüsselung unterstützen, stellten Ende Juli 2014, gemessen an IP-Adressen, 1,31 Prozent der https- und 1,28 Prozent der SMTP-Server weiterhin ein Sicherheitsrisiko dar.

„Die Auswertungen zeigen deutlich, dass professionell gewartete Server schnell aktualisiert werden. Ein Großteil der Server in Österreich ist mittlerweile in Sachen *Heartbleed* geschützt“, erklärt Lendl. Das größte Sicherheitsrisiko stellen nach wie vor Server in kleinen und mittelständischen Unternehmen oder Vereinen dar, die schlecht oder nicht gewartet werden. „Der Schaden für den Einzelnen hält sich zwar in Grenzen, aber solche Websites können von Dritten als Werkzeug für Angriffe verwendet werden“, sagt Lendl.

IT-Infrastruktur-Pflege. „Heartbleed ist ein Beispiel dafür, dass man als IT-Verantwortlicher die Pflicht hat, seine Systeme laufend zu pflegen und auf dem aktuellsten Stand zu halten“, sagt Wolfgang Breyha, Postmaster und Hauptverantwortlicher des Mailsystems der Universität Wien. „So schnell *Heartbleed* publik geworden ist, fast genauso schnell hat es bereits Patches und Anleitungen gegeben, um das Sicherheitsleck zu stopfen.“ *Heartbleed* war problematisch, weil aktuelle Builds eingesetzt wurden. Die meisten, veralteten, Versionen hatten diese Sicherheitslücke nicht. Das Auftreten der Sicherheitslücke wird in diesem Fall durch aktualisierte Software nicht verhindert. Nach Entdecken der Lücke ist Aktualisieren jedoch wichtig, um diese zu beseitigen. Mit dem Austausch der fehlerhaften Software alleine ist es nicht getan. Administratoren betroffener Websites oder E-Mail-Anbieter müssen auch neue Schlüssel und neue Zertifikate erstellen. Zertifikate werden in Browsern oder E-Mail-Programmen der Anwender gespeichert, um einen verschlüsselten Zugang zu verifizieren.

Heartbleed ermöglicht es, die kryptografischen Schlüssel eines Servers auszulesen, der in Zertifikate integriert ist. Das birgt die Gefahr, dass Kriminelle den SSL-Schlüssel erlangen und damit eine gefälschte Webseite aufsetzen. Sie können Opfer auf diese Seite locken, indem sie ihnen vortäuschen, es sei eine echte, abgesicherte Seite. Der Betreiber einer betroffenen Website oder ein E-Mail-Anbieter muss seine Kunden informieren und ihnen nahelegen, ihre Kennwörter zu ändern.

Verschlüsselung. Vorfälle wie *Heartbleed* oder der Diskurs rund um die Enthüllungen von Edward Snowden haben aus Sicht der IT-Experten auch ihre positiven Seiten: Im Umgang mit Privacy und Verschlüsselung kommt es bei Anwendern und Anbietern zu positiven Bewegungen. Der Schutz eigener Daten und der Privatsphäre im Internet haben für viele Nutzer zunehmende Priorität.

Immer mehr E-Mail-Anbieter verschlüsseln Nachrichten zur sicheren Übertragung. Laut dem *Google*-Transparenzbericht werden mit Stand Juli

FOTO: EGON WEISSHEIMER

2014 bereits knapp drei Viertel aller ausgehenden Nachrichten von *Gmail* an andere Anbieter verschlüsselt übermittelt. Eingehend ist dies bereits bei jeder zweiten Mail der Fall.

Die Experten von *CERT.at* empfehlen den IT-Anwendern, egal ob beruflich oder privat, bei der Auswahl von E-Mail- und Web-Service-Anbietern darauf zu achten, dass diese verschlüsselte Datenübertragung eingesetzt wird – und dies gegebenenfalls auch einzufordern.

Mit *Heartbleed* rückt aus Sicht von *CERT.at* noch ein weiteres Thema in den Vordergrund: Die zunehmende IT-Sicherheitsgefährdung in Verbindung mit dem „Internet der Dinge". Aaron Kaplan, IT-Sicherheitsexperte bei *CERT.at,* warnt: „Der Vorstoß der IT in alle Bereiche des täglichen Lebens setzt sich unaufhaltsam fort. Immer mehr Geräte sind miteinander vernetzt und kommunizieren miteinander." Man kann mit einem Smartphone Licht, Heizung, Sauna, Kühlschrank oder Toaster steuern. Da seien regelmäßige Programm-Updates immer wichtiger.

Better-Crypto. Um Betreibern von Mail- und Webservern beim richtigen Set-up ihrer IT-Systeme zu unterstützen, hat sich eine Gruppe IT-Sicherheitsexperten zusammengeschlossen und einen Leitfaden für Systemadministratoren erstellt, wie sie ihre Web- und Mailserver verschlüsseln können. Die *Better-Crypto*-Expertengruppe gibt darin einen Überblick über den aktuellen Stand der Technik in Sachen Verschlüsselung und will vor allem weniger erfahrene Systemadministratoren mit vorgeschlagenen Einstellungen dabei unterstützten, ihre Systeme mit einfachen Mitteln sicherer zu machen.

„Wer nicht verschlüsselt, macht sich zum Freiwild fürs Abhören", sagte Pepi Zawodsky, Mitautor des Leitfadens. „Uns ist wichtig, dass alle Administratoren überall Verschlüsselung einsetzen. Zudem können Sicherheitsmaßnahmen oft durch wenige Zeichen in den Settings deutlich verbessert werden." Schlechte Verschlüsselung sei besser als keine und würde es Geheimdiensten erschweren, an Daten zu gelangen. *Siegbert Lattacher*

Information: www.cert.at; Informationen über die Better-Crypto-Expertengruppe und Download des Leitfadens: https://bettercrypto.org