Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Was ist Verschlüsselung
- Stationäre Verschlüsselung
- Verschlüsselung des Datenverkehrs

Verschlüsselung

Was ist Verschlüsselung?

Sicher haben Sie schon oft den Begriff "Verschlüsselung" gehört und dass Sie davon Gebrauch machen sollen um sich und Ihre Informationen zu schützen. Das Konzept dahinter ist jedoch eher kompliziert. Verschlüsselung kann Sie zudem nicht vor allem schützen, ihre Anwendung hat Grenzen. In diesem Newsletter erklären wir mithilfe einfacher Begriffe, was Verschlüsselung ist, warum Sie verschlüsseln sollten und worauf man dabei achten muss.

Gastautor

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) ist ein Berater aus der Nähe von Washington, DC. Er verantwortet den Kurs „Mobile Device Security and Ethical Hacking„ (SEC575) des SANS Institute und ist Autor des Kurses „Incident Response Team Management" (MGT535).

Sie haben eine gewaltige Menge sensibler Dokumente auf Ihren elektronischen Geräten, darunter Finanzdokumente, Fotos, E-Mails, vielleicht sogar medizinische Daten. Wenn eines Ihrer Geräte verloren geht oder gestohlen wird, können diese Informationen ggfs. von Unberechtigten eingesehen werden. Da Sie mithilfe Ihrer technischen Geräte zudem bestimmt auch sensible Onlinetransaktionen wie z.B. Onlinebanking oder Bezahlvorgänge beim Onlineshopping abwickeln, könnten Cyberkriminelle, die Ihre Onlineaktivitäten überwachen, auch Zugang zu Ihrem Bankkonto oder Ihre Kreditkartendaten erlangen und diese stehlen. Verschlüsselungstechnologien schützen Sie in all diesen Situationen, indem sie sicherstellen dass Unberechtigte keinen Zugriff auf Ihre Informationen haben und diese auch nicht manipulieren können.

Unverschlüsselte Informationen werden auch als Klartext bezeichnet, um zu verdeutlichen, dass jedermann sie einfach lesen oder darauf zugreifen kann. Verschlüsselung wandelt diese Informationen in ein unlesbares Format um, den Kryptotext oder Chiffrentext. Verschlüsselung basiert dabei auf komplexen mathematischen Operationen und einem einzigartigen Schlüssel. Dieser Schlüssel verhindert oder ermöglicht den Zugriff auf Ihre Informationen, genau so wie ein echter Schlüssel eine Tür zu- oder aufschließen kann. Ein gängiges Beispiel eines solchen Schlüssels ist das Passwort, mithilfe dessen jeder, der es kennt, auf damit geschützte Informationen zugreifen kann. Um Ihre verschlüsselten Informationen zu schützen ist es daher essentiell, den dazugehörigen Schlüssel zu schützen. Bei Verschlüsselung unterscheidet man zwei grundverschiedene Zustände: Verschlüsselung von stationären Daten, z.B. auf Ihrem Laptop, und Transportverschlüsselung, z.B. während der Datenübertragung im Internet.

Verschlüsselung stationärer Daten

Das primäre Ziel von stationärer Verschlüsselung ist der Schutz Ihrer Informationen im dem Fall, dass Ihr Computer oder der Datenträger verloren geht oder gestohlen wird. Vor 15 Jahren war das noch kein Problem, als Computer

Verschlüsselung

noch große, unhandliche Geräte waren die nur schwer bewegt werden konnten. Heutige Laptops sind dagegen Fliegengewichte, und Mobilgeräte wie Smartphones sind noch viel leichter. Diese Geräte sind sehr leistungsstark und halten eine sehr große Menge an Informationen, sind jedoch auch sehr leicht zu verlieren. Zudem gibt es kleine Datenträger wie USB-Sticks, SD-Karten und DVDs, die ebenso leicht abhanden kommen können. Eine gängige Technik zur Verschlüsselung von Informationen auf Datenträgern wird Full Disk Encryption (FDE) bzw. Festplatten- oder Datenträgerverschlüsselung genannt. Dabei ist automatisch alles auf dem Gerät verschlüsselt und Sie müssen nicht unterscheiden, was verschlüsselt werden soll und was nicht. Die meisten aktuellen Betriebssysteme haben eine solche Funktion bereits eingebaut, die Sie nur noch aktivieren müssen. Bei Mac OS X z.B. nennt sie sich FileVault und einige Versionen von Windows enthalten Bitlocker. Wenn Ihr Computer eine solche Datenträgerverschlüsselung bietet, raten wir dringend davon Gebrauch zu machen. Viele Mobilgeräte wie Smartphones unterstützen ebenfalls die Vollverschlüsselung ihres internen Speichers. So aktiviert iOS, das Betriebssystem von iPhones und iPads, automatisch die Verschlüsselung sobald ein Passwortschutz eingerichtet wurde. Fragen Sie die PC-Betreuung bzw. den Helpdesk in Ihrem Unternehmen, ob Ihr Computer eine Vollverschlüsselung bietet. Als Privatnutzer können Sie sich an die Hotline ihres Computerherstellers oder –verkäufers wenden, oder in der mitgelieferten Anleitung nachlesen.

Verschlüsselung ist ein sehr guter Weg Ihre Informationen zu schützen, sie ist aber nur so stark wie der gewählte Schlüssel.

Verschlüsselung des Datenverkehrs

Informationen sind auch verwundbar, wenn sie übertragen werden. Wenn Daten nicht verschlüsselt sind können sie unberechtigt mitgelesen und sogar während des Transports manipuliert werden. Daher sollten Sie unbedingt darauf achten, dass sensible Aktionen wie Onlinebanking, das Versenden von E-Mails und auch der Zugriff auf Soziale Netzwerke über verschlüsselte Verbindungen erfolgen. Die hierfür gängigste Methode ist HTTPS. Das bedeutet, dass sämtliche Daten, die zwischen Ihrem Internetbrowser und einer Webseite ausgetauscht werden, verschlüsselt sind. Prüfen Sie, ob die Adresszeile mit https:// beginnt, ein Schloss in der Adresszeile zu sehen ist oder sie grün eingefärbt ist. All dies sind Zeichen, dass die Kommunikation verschlüsselt abläuft. Abhängig vom verwendeten Browser und der aufgerufenen Webseite können Sie ggfs. auch alle drei gleichzeitig sehen. Wann immer Sie sich mit einem öffentlichen WLAN verbinden, sollten Sie zudem auch darauf achten, wo immer möglich verschlüsselte Verbindungen zu nutzen. Richten Sie Ihr E-Mail Programm so ein, dass E-Mails über eine verschlüsselte Verbindung übertragen werden. Aktuelle E-Mail Programme haben dies längst eingebaut und auf den Hilfe-Seiten Ihres E-Mail Anbieters finden Sie die benötigten Daten für die korrekte Einrichtung.

© The SANS Institute 2014

Verschlüsselung

Verschlüsselung richtig einsetzen

Unabhängig davon, welche Art der Verschlüsselung Sie nutzen, gibt es einige Punkte zu beachten, um die sichere Anwendung zu gewährleisten:

- Die Verschlüsselung ist nur so stark wie der genutzte Schlüssel. Wenn jemand einfach Ihr Passwort erraten oder beim Eingeben mitlesen kann, hat er wahrscheinlich schon Zugriff auf Ihre Daten. Sie müssen den Schlüssel unbedingt geheim halten!
- Wenn Ihr Schlüssel mit einem Passwort oder Passwortsatz geschützt ist, stellen Sie sicher dass es ausreichend lang ist und dass Sie es nicht vergessen. Wenn dies eintritt, werden auch Sie keinen Zugriff auf Ihre eigenen Daten mehr haben.
- Die Verschlüsselung ist nur so stark wie die Sicherheit Ihres Computers. Wenn Ihr Computer mit Schadsoftware befallen ist, haben Cyberkriminelle wahrscheinlich die Möglichkeit die Verschlüsselung zu umgehen. Halten Sie daher die Programme auf Computer und Smartphone unbedingt aktuell.
- Wenn Sie aus verschiedenen Möglichkeiten der Verschlüsselung wählen können, sollten Sie immer die stärkste wählen.

Weiterführende Informationen

Mac OS X Filevault:	http://support.apple.com/kb/HT4790?viewlocale=de_DE
iOS Verschlüsselung:	http://support.apple.com/kb/ht4175?viewlocale=de_DE
Android Verschlüsselung:	http://www.spiegel.de/netzwelt/web/smartphones-android-geraete-verschluesseln-a-946169.html
Windows Verschlüsselung:	http://windows.microsoft.com/de-de/windows/protect-files-bitlocker-drive-encryption
Absicherung Ihres Computers:	http://www.securingthehuman.org/ouch/2012#december2012
Passwortverwaltung:	http://www.securingthehuman.org/ouch/2013#october2013

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

OUCH! wird durch das SANS Securing The Human Programm herausgegeben und unter der Creative Commons BY-NC-ND 3.0 Lizenz vertrieben. Die Erlaubnis zur Weitergabe dieses Newsletters oder Verwendung in einem Weiterbildungsprogramm wird gewährt, solange der Newsletter unverändert bleibt. Für Übersetzungen und weitere Informationen kontaktieren Sie bitte ouch@securingthehuman.org.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus