Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Was ist Verschlüsselung?
- Was können Sie verschlüsseln?
- So machen Sie es richtig.

Verschlüsselung

Was ist Verschlüsselung?

Sie haben sicher schon einmal den Begriff „Verschlüsselung“ gehört und wie man diese für den eigenen Schutz und den seiner Informationen nutzen soll. Die Nutzung von Verschlüsselung ist oft nicht leicht verständlich, um so wichtiger ist es, dass Sie auch ihre Grenzen kennenlernen. In dieser Ausgabe wollen wir Ihnen in einfachen Worten erklären, was Verschlüsselung ist, wie sie Sie schützen kann und wie man sie richtig anwendet.

Gastautor

Als Sicherheitsexpertin und Projektleiterin betreut Francesca Bosco (**@francibosco**) Projekte rund um die Themen Cybercrime, Cybersecurity und Missbrauch jeglicher technischer Geräte. Sie arbeitet für das „Interregional Crime and Justice Research Institute“ der Vereinten Nationen und ist Mitgründerin des „Tech and Law Centers“.

Auf Ihren Geräten lagern große Mengen an sensiblen Informationen, wie z.B. persönliche Dokumente, Bilder und E-Mails. Wenn Sie Ihr Gerät verlieren oder es gestohlen wird, könnte jeder, der es in die Hände bekommt, auf diese sensiblen Informationen zugreifen. Sollten Sie zudem noch Bankgeschäfte über Ihren PC oder Ihr mobiles Gerät abwickeln, könnten zusätzlich auch Ihre Zugangsdaten für Ihr Konto oder Kreditkartendaten abhanden kommen. Um dem vorzubeugen, sollten Sie die Daten auf Ihrem Gerät verschlüsseln, so dass unberechtigte Personen Ihre Daten nicht einsehen oder ändern können.

Verschlüsselung wird schon seit tausenden von Jahren genutzt. Bis heute wurde die Verschlüsselungstechnologie ständig weiterentwickelt, erfüllt aber immer noch den selben Zweck - sie soll sicherstellen, dass eine geheime Nachricht von einem Ort zum anderen transportiert wird und nur berechtigte Personen die Nachricht einsehen können. Unverschlüsselte Informationen werden auch Klartext genannt. Dies bedeutet, dass sie jedermann lesen oder darauf zugreifen kann. Verschlüsselung wandelt diese Informationen in ein nicht lesbares Format um, auch Chiffretext genannt. Die heutigen Verschlüsselungsmethoden nutzen komplexe mathematische Operationen und einen einzigartigen Schlüssel, um Ihre Informationen in Chiffretext zu verwandeln. Nur der Schlüssel erlaubt Ihnen Zugriff auf Ihre Informationen. In den meisten Fällen handelt es sich dabei um ein Passwort.

Was können Sie verschlüsseln?

Es gibt zwei Arten von Daten die Sie verschlüsseln können. Ruhende Daten (z.B. Daten die auf Ihrem Mobilgerät gespeichert sind) oder in Bewegung befindliche Daten (z.B. E-Mails oder Nachrichten die Sie empfangen).

Verschlüsselung

Um Ihre ruhenden Daten im Falle eines Verlustes oder Diebstahls Ihres Computers oder Mobilgerätes zu schützen, ist es unabdingbar, diese Daten zu verschlüsseln. Heutige Geräte sind extrem leistungsfähig und beinhalten eine riesige Menge Informationen, sind gleichzeitig aber auch leicht zu verlieren. Auch andere Medien können wichtige Daten enthalten, z.B. USB Sticks oder externe Festplatten. Festplattenverschlüsselung (Full Disk Encryption, FDE) ist eine verbreitete Technologie die ein Laufwerk in Ihrem System vollständig verschlüsselt. Alles, was sich darauf befindet, ist damit automatisch für Sie verschlüsselt, Sie müssen nicht entscheiden was Sie verschlüsseln wollen und was nicht. Die meisten Computer bringen heutzutage die Fähigkeit zur Festplattenverschlüsselung mit, aber Sie müssen sie manuell aktivieren. Auf Mac Computern wird die Funktion FileVault genannt, auf Windows Computern hingegen können Sie Bitlocker zur Laufwerksverschlüsselung nutzen. Die meisten Mobilgeräte unterstützen ebenfalls eine Vollverschlüsselung. iOS auf iPhones und iPads aktiviert diese automatisch, sobald ein Passwort für das Gerät vergeben wurde. Seit Android 6.0 (Marshmallow) fordert auch Google, dass Vollverschlüsselung standardmäßig aktiviert ist, vorausgesetzt dass die Hardware bestimmte Mindestkriterien erfüllt.

Verschlüsselung ist eine wirkungsvolle Methode Ihre Daten zu schützen, aber sie ist nur so stark wie der Schlüssel, den Sie dafür verwenden.

Informationen sind auch während der Übertragung verwundbar. Wenn die Daten nicht verschlüsselt sind, können sie ausgelesen, verändert oder abgefangen werden. Daher sollten Sie sicherstellen, dass jede sensible Onlinetransaktion und -verbindung verschlüsselt abläuft. Eine geläufige Form der Online-Verschlüsselung ist HTTPS. Dabei ist der komplette Datenverkehr zwischen Ihrem Browser und der HTTPS-gesicherten Webseite verschlüsselt. Sie erkennen das daran, dass die Adresszeile mit https:// beginnt, ein Schlosssymbol in der Adresszeile erscheint oder die Zeile grün eingefärbt wird. Ein weiteres Beispiel ist das Versenden oder Empfangen von E-Mail. Die meisten E-Mail-Programme bieten Möglichkeiten zur verschlüsselten Übertragung, die Sie einmalig aktivieren müssen. Ein drittes Beispiel ist die verschlüsselte Übertragung von Daten zwischen Chat-Partnern, wie sie z.B. iMessage, Threema, Signal, WhatsApp oder Telegram bietet. Apps wie diese nutzen sogenannte Ende-zu-Ende Verschlüsselung, die verhindert, dass unberechtigte Dritte während der Übertragung von einem System auf das andere auf die Daten zugreifen. Somit können nur Sie und die Personen mit denen Sie kommunizieren lesen, was geschrieben wurde.

So machen Sie es richtig

Um sicher zu gehen, dass Sie bei der Verwendung von Verschlüsselung wirklich geschützt sind, ist es an erster Stelle wichtig, diese korrekt einzusetzen.

Verschlüsselung

- Die Verschlüsselung ist immer nur so stark wie der Schlüssel. Wenn jemand Ihren Schlüssel herausfindet oder darauf Zugriff bekommt, hat er Zugriff auf die damit verschlüsselten Daten. Schützen Sie Ihre Schlüssel! Wenn Sie Passwörter für Ihre Schlüssel benutzen, stellen Sie sicher, dass es sich um starke, einzigartige Passwörter handelt. Je länger die Passwörter sind, desto schwieriger ist es für einen Angreifer sie durch schiere Rechenleistung zu knacken. Vergessen Sie die Passwörter aber nicht, denn ohne den Schlüssel können Sie selbst auch nicht mehr auf die Informationen zugreifen. Wenn Sie sich nicht alle Passwörter merken können, empfehlen wir die Nutzung eines Passwortsafes.
- Die Verschlüsselung ist, nur so stark wie die Sicherheit Ihrer Geräte. Wenn Ihr Gerät bereits mit Schadprogrammen infiziert ist können Cyberangreifer die Verschlüsselung umgehen. Daher ist es so wichtig, dass Sie Schritte zur Absicherung Ihrer Geräte ergreifen, darunter die Nutzung von Antivirusprogrammen, das Einspielen aller Aktualisierungen und die Nutzung starker Passwörter.
- Viele Mobil-Apps bieten nun auch starke Verschlüsselung zum Schutz Ihrer Daten und Kommunikation an. Wenn eine App oder ein Programm, dass Sie einsetzen wollen, dies nicht bietet, sollten Sie sich nach einer besseren Alternative umsehen.

Weiterführende Informationen

Verschlüsselung einfach erklärt (Video):	http://www.spiegel.de/video/daten-verschluesseln-einfach-erklaert-video-1656682.html
Starke Passwörter:	https://securingthehuman.sans.org/ouch/2015#april2015
Passwort Manager bzw. Passwort-Safe:	https://securingthehuman.sans.org/ouch/2015#october2015
Schadprogramme:	https://securingthehuman.sans.org/ouch/2016#march2016
Absicherung Ihres neuen Tablets:	https://securingthehuman.sans.org/ouch/2016#january2016

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 securingthehuman.sans.org/ouch/archives.

Deutsche Ausgabe

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

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