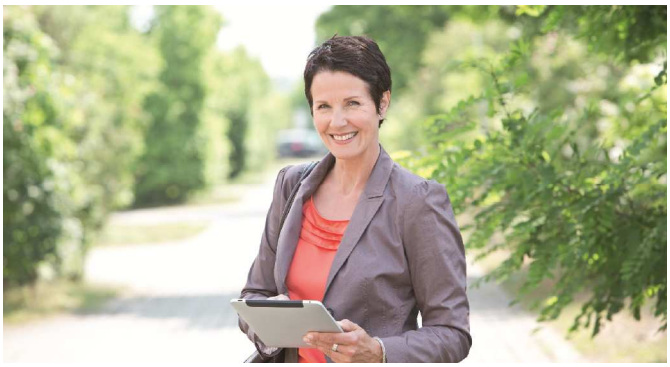
DATEV Zukunft gestalten. Gemeinsam.

Aktuelles zum Datenschutz



Ausgabe 05 | Oktober 2015

Sehr geehrte Damen und Herren,

Stellen Sie sich vor, Sie erhalten diesen Anruf: „Hallo hier ist Herr Müller von Microsoft. An ihrem PC muss eine aktuelle Sicherheitssoftware installiert werden.“ Was Sie nicht ahnen – der Anrufer arbeitet nicht bei diesem Softwarehersteller sondern startet einen sog. Social Engineering Angriff auf Ihr Unternehmen. Bevorzugt erfolgen solche Angriffe über das Telefon, da Angreifer so ihre wahre Identität verschleiern und eine gewisse Distanz zum Opfer wahren können. In einigen Fällen baut der Angreifer eine persönliche Beziehung zum Opfer auf, indem er mehrere Male anruft und erst nach einiger Zeit Fragen zu bestimmten Informationen stellt. Dabei würde ein gewiefter „Social Engineer“ niemals direkt auflegen, nachdem er die gewünschte Information erhalten hat. Denn der Anrufer erinnert sich zumeist an den Anfang und das Ende des Gesprächs und nicht an einzelne, vermeintlich nebensächliche Fragen, die zwischendurch gestellt wurden. Eine aktuelle Vorgehensweise des Social Engineerings wird im Folgenden näher vorgestellt.

Viel Spaß bei der Lektüre wünscht Ihnen

Markus Seifert, DATEV-Consulting

Vorsicht: Anrufer geben sich als Microsoft-Techniker aus

In letzter Zeit kommt es vermehrt zu Anrufen von angeblichen Microsoft Mitarbeitern. Die Betrüger rufen Unternehmen und private Haushalte an und verlangen, dass auf dem Computer des Angerufenen dringend eine Sicherheitssoftware installiert werden muss. Der Anrufer überzeugt sogar durch internes Wissen über den PC, denn er sagt er kenne die Lizenznummer des PC-Systems. Um den Angerufenen zu überzeugen, bittet er diesen folgende Befehle auszuführen:

- Klicken Sie auf Start,
- Geben Sie „cmd“ ein und drücken Sie „Enter“,
- Geben Sie „assoc“ ein,
- Dann erscheint folgende Zeile: ZFSendToTarget=CLSID\{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}

Jedoch ist diese Nummer auf jedem PC identisch. Nach dieser überzeugenden Vorstellung des angeblichen Microsoft-Technikers bittet dieser den Anwender eine Fernwartungssoftware, z.B. TeamViewer, zu installieren, um so den angeblichen Microsoft-Techniker Zugriff auf den PC zu gewähren. Natürlich manipuliert der Abzocker daraufhin das System, indem er verschiedenste bösartige Aktionen durchführt. Für diese „Dienstleistung“ wird im Rahmen des Gespräches die Zahlung einer Servicepauschale in Höhe von 65 Euro eingefordert. Zudem werden oft auch die Kreditkartendaten verlangt.

Was können Sie dagegen tun? Der eigentliche Mangel ist nicht eine fehlerhafte IT-Technik oder eine unzureichend gesicherte Anwendung. Das eigentliche Problem entsteht vor dem Rechner und kann nur durch geeignete organisatorische Maßnahmen in Verbindung mit einer entsprechenden Sensibilisierung der IT-Nutzer vor fehlerhaften Handlungen vermieden werden. Wir empfehlen daher, zusammen mit Ihrem Datenschutzbeauftragten mögliche Angriffsszenarien zu analysieren und geeignete Vorkehrungen / Regelungen zum Schutz Ihrer IT zu treffen und diese Ihren Mitarbeitern regelmäßig und verständlich zu vermitteln.

IT-Sicherheitsgesetz: Das sind die neuen Anforderungen

Haben Sie es mitbekommen, am Freitag, den 12. Juni 2015 hat der Bundestag das von der Bundesregierung vorgelegte IT-Sicherheitsgesetz beschlossen. Das Gesetz legt für Betreiber sogenannter „kritischer Infrastrukturen" ein Mindestniveau an IT-Sicherheit fest die den Schutz der IT und damit die Sicherstellung der Grundversorgung der Bevölkerung gewährleisten sollen. Diese beinhaltet eine Meldepflicht von IT-Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnologie (BSI). Soweit so gut. Wer genau ist hiervon betroffen, und welche Pflichten bestehen jetzt im konkreten?

- Betreiber von Webangeboten sind verpflichtet, ausreichende, dem Stand der Technik entsprechende technische und organisatorische Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme zu ergreifen.
- Telekommunikationsunternehmen haben, neben der Pflicht ihre Systeme ausreichend gegen Cyberangriffe zu sichern die Verpflichtung, Kunden über mögliche Missbräuche ihrer Anschlüsse zu informieren.
- Die höchsten Anforderungen stellt das IT-Sicherheitsgesetz jedoch an die Betreiber kritischer Infrastrukturen (siehe https://www.bsi.bund.de/DE/Themen/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html). Diese müssen sich, neben der Schaffung ausreichender dem Stand der Technik entsprechender Sicherheitsmaßnahmen, alle 4 Jahre einer Evaluation dieser Maßnahmen unterziehen.
- Herzstück des IT-Sicherheitsgesetzes sind neben den gesetzlichen Vorgaben zur Einrichtung angemessener technischer und organisatorischer Maßnahmen zum Schutz von IT-Systemen die diversen Meldepflichten über IT-Sicherheitsvorfälle an das BSI, welches künftig als zentrale Melde- und Aufsichtsstelle fungieren wird.

Datenschutz-Tipp: Sicher surfen, 7 Datenschutz Add-Ons für Firefox

Cookies, Skripte und andere Trackingmethoden ermöglichen eine nahezu lückenlose Verfolgung Ihrer Internetnutzung. Verschiedene kostenlose Browser-Add-Ons für Firefox machen solche Trackingmaßnahmen transparent und können diese einschränken:

- **Ghostery:** erkennt die auf einer Webseite eingesetzten Tracking-Tools und bietet die Möglichkeit, diese zu blockieren.
- **BetterPrivacy:** schützt vor Flash-Cookies und bietet die Möglichkeit, diese zu entfernen (Flash-Cookie = browserunabhängige, lokal am PC gespeicherte und von der browserseitigen Löschung nicht erfasste Cookies).
- **Flashblock:** verhindert das automatische Ausführen von Flashanimationen auf Webseiten.
- **Google search link fix:** der ursprüngliche Link wird wiederhergestellt und eine Aufzeichnung durch Google verhindert. (Bei Google-Suchen wird der angezeigte Link zu den Zielseiten von Google verändert. Die veränderte URL beginnt mit "www.google". Google zeichnet so auf, welche Seiten über die Google-Suche besucht wurden.)
- **HTTPS everywhere**: ersetzt unverschlüsselte HTTP-Anfragen durch verschlüsselte HTTPS-Anfragen.
- **NoScript:** JavaScripts werden auf den Webseiten unterbunden.
- **Random Agent Spoofer:** verschleiert und verfälscht die an eine Webseite automatisch gesendeten Informationen (z.B. IP-Adresse, Webbrowser-Version, Betriebssystem etc.).

Gerne unterstützt Sie Ihr Datenschutzbeauftragter!

Weitere Informationen erhalten Sie auf: www.datev.de/datenschutz und www.datev.de/consulting
Kontakt: consulting@datev.de – Telefon +49 911 319-7051

Kennen Sie schon unser Seminar-Angebot? Informationen dazu erhalten Sie auf:
www.datev.de/chef-seminare | Office-Management und IT