Informationssammlung zur Unternehmenssicherheit

Liebe Azubis der Abteilung Unternehmenssicherheit. In den letzten Wochen kam es vermehrt zu Anfragen von Mitarbeitern die sich über die Sicherheitsrisiken in unserem Unternehmen informieren wollten. Um bei solchen Gesprächen den Überblick zu behalten haben wir eine Übersicht über die gängigsten Gefahren in IT Systemen erstellt. Diese kann bei Gesprächen als Leitfaden genutzt werden.

Beste Grüße von eurer

IT-Sicherheitsabteilung

Die verschiedenen Formen unerwünschter Post

Man unterscheidet zwischen verschiedenen Formen von unerwünschter (digitaler) Post.

1. Phishing Mail
2. Hoax Mail
3. Spam Mail

Folgende Erkennungsmerkmale können auf unerwünschte Post hindeuten. Bitte besonders darauf achten digitale Post mit folgenden Merkmalen nicht zu öffnen:

1. Der Absender stimmt nicht
2. E-Mail Anhänge sind verdächtig
3. Mahnung, Inkasso oder Anwalt
4. Unternehmen verlangen keine Daten per Mail
5. E-Mail Text ist verdächtig
6. Unrealistischer Zeitdruck
7. Den Header bzw. den Weg von E-Mails richtig auslesen

Sollte es tatsächlich zu einem Fall von unerwünschter Post gekommen sein sind folgende Vorgehensweisen zu beachten:

1. Auf keinen Fall auf die Mail antworten
2. Wenn es sich um einen handfesten Betrugsversuch handelt – bei der Polizei o.Ä melden damit andere Nutzer auch gewarnt sind
3. Spam-Filter aktivieren
4. HTML-Sicht ausstellen – Da Mails Codes und Skripte enthalten
5. Im Outlook unter Trust Center „nur Text“ für die Mails aktivieren. Das sieht bei HTML schräg aus dient jedoch sehr zur Sicherheit
6. Niemals unbekannte Anhänge öffnen oder Dateien wie .exe ausführen

Ausarbeitung von Heiko Forro, Ekrem Güler, Maximilian Rädlein und Lasse Riegel

Falsche Antivirussoftware

Vermeintliche Antivirus-Software, die eigentlich keine nützliche Funktion hat.

Wird meist durch Popups angeboten, die anzeigen, dass der Computer vermeintlich gefährdet oder bereits von Viren befallen ist.

Lädt man das Programm runter, tut es meist so, als würde es die Festplatte untersuchen und fordert nach Abschluss der Untersuchung dazu auf, das Programm zu kaufen um die gefunden Viren (meist sehr hohe Anzahl) zu beseitigen. Oft tauchen solche Popups auf, wenn man sich absichtlich oder unabsichtlich auf zwielichtigen Websites bewegt oder wenn man zuvor ausversehen potentiell unerwünschte Software installiert hat.

Die Programme dienen meist dazu Kreditkarten- oder Zahlungsinformationen zu sammeln oder u. U. sogar auf direktem Wege Geld zu kassieren. Grundsätzlich sollte man immer misstrauisch bei Popups sein und sich stattdessen lieber bewusst über Anti-Viren-Software informieren und diese direkt bei namhaften Herstellern beziehen. Egal ob kostenpflichtig oder kostenlos.

Potentiell unerwünschte Programme (PuP)

Die Programme werden meist bei kostenlosen Programmen als „unerwünschte Zugabe“ mitinstalliert, wenn man nicht genau hinschaut und bei der Installation zu schnell auf Weiter klickt.

Meist handelt es sich um Browser-Toolbars oder „Suchmaschinen-Optimierer“, die die Suchmaschinen zugunsten von Werbetreibenden optimieren, aber niemals zugunsten des Benutzers. Oft werden Ergebnisse angepasst oder auch nur die Links, wodurch man dann plötzlich auf unerwünschten Kasino-Seiten landet oder auf einer Seite, die einem Malware anbietet.

Häufig wird auch bei seriöser Software, wie z. B. bei kostenlosen Adobe Produkten solche Software angeboten. Hier ist jedoch auch die unerwünschte Software oft auch einigermaßen seriös und auch einfach zu entfernen. Anders ist das bei der unerwünschten Software, die von dubiosen Herstellern angeboten wird. Hier fehlen oft Deinstallations-Routinen oder diese sind fehlerhaft, sodass Reste der Software erhalten bleiben und sich beim nächsten Neustart des PCs automatisch wieder installieren. Oft können diese Reste dann nur mit einer gründlichen System- und Registry-Bereinigung oder gar einer kompletten Neuinstallation des Betriebssystems installiert werden.

Nicht selten führen genau solche PuP zu den oben aufgeführten Popups, die zur Installation von falscher Antivirus-Software führen.

Schadprogramme

Schadprogramme bringen absichtlich schädliche Wirkung oder missbräuchliche Nutzung auf Ihr System, nicht zu verwechseln mit fehlerhaft programmierter Software. Diese ist nicht absichtlich schädlich.

Verschiedene Arten von Schadsoftware sind:

Trojanische Pferde (Trojaner) – also gut getarnte Software, Viren, sowie Würmer, die sich selbstständig vermehren. Cyber-Kriminelle sind selten Einzeltäter, meist organisiert und international verstreut. Oft sind sie politisch oder finanziell motiviert. Es läuft ein Wettlauf zwischen Schadprogrammentwicklern und Sicherheitsprogrammentwicklern – alles wird komplexer. Gefährdet sind prinzipiell alle softwaregesteuerten und vernetzten Systeme. Guter Schutz ist wichtig, z.B. durch Antivirenprogramme, abgeschottete Netzwerke durch Router und ggf. VLANs, gute Rechtekontrolle mit Passwörtern und eingeschränkte Konten, sowie geschulte Anwender. Schadprogramme gelangen nicht nur durch Backdoors, sondern auch getarnt als Mailanhang oder in ungefährlich aussehender Software aufs System. Gesteuert werden sie von außen durch Command and Control Servern.

Botnetze

Von Botnetzen spricht man dann, wenn sehr viele PCs – meist mehrere Tausend – per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden. Diese Zusammenschlüsse werden vom Nutzer meinst nicht bemerkt weil die Bandbreite der Breitbandanschlüsse mittlerweile so hoch ist, dass der zusätzliche Traffic nicht wahrgenommen wird.

Wie werde ich durch ein Botnetz infiziert?
Hacker übernehmen zunächst meinst ein UNIX Serversystem um ihr Botnetz zentral zu steuern. Dieser Server befällt daraufhin automatisch weitere Hosts die mit dem Internet verbunden sind. Das alles passiert voll automatisch.

Wofür werden Botnetze genutzt?
Botnetze werden vor allem für DDOS Angriffe genutzt. Durch die große Anzahl von Host in dem Botnetz können die Systeme von großen Firmen durch gleichzeitiges anpingen von tausenden infizierten Geräten leicht lahmgelegt werden. Mediatheken, Steuerungen für Atomkraftwerke, Datenserver oder Krankenhäuser können durch Botnetzangriffe lahmgelegt werden.

Botnetze werden also genutzt, um die Infrastruktur von Unternehmen oder sogar ganzen Ländern zu schwächen. Gegen Bezahlung vermieten Hacker ihre Botnetze an andere.