Neue Gefahren aus dem Internet erfordern neue Maßnahmen

Deutlich erhöhtes Bedrohungs- und Schadensrisiko

Die Gefährdung von IT-Systemen durch externe Bedrohungen hat in den letzten Monaten signifikant zugenommen. Nicht nur die Zahl der Bedrohungen, auch die Qualität von z.B. Fake-Mails oder Phishing Angriffen hat deutlich zugenommen. Umfangreiche Hintergrundinformationen hierzu liefert u.a. auch der Bericht zur „Lage der IT-Sicherheit in Deutschland 2015“ des BSI (Bundesamt für Sicherheit in der Informationstechnik)[1].

Auch wir haben in den letzten Monaten eine steigende Zahl von Sicherheitsvorfällen mit direkter Auswirkung auf den produktiven Betrieb der IT-Systeme feststellen müssen. Insbesondere die sogenannten „Crypto-Viren“ sorgen für Beeinträchtigungen oder sogar Ausfälle von Systemen und Verlust von Daten. Technische Gegenmaßnahmen können einen guten Teil der Problematik verhindern, jedoch ist auch die Information und Sensibilisierung der Anwender ein unbedingtes Muss, um Schaden für das Unternehmen abzuwenden.

Wir möchten Ihnen fünf Maßnahmen vorstellen und nahelegen:

Benutzerrechte mit Augenmaß vergeben

Problem: Ein historisch gewachsenes Problem ist die Vergabe von administrativen Rechten an Standardbenutzer-Konten. Dadurch erhält ein durch Schadprogramme („Malware“) befallenes Benutzerkonto weitreichende Rechte, um Schäden an Systemen und Daten hervorrufen zu können. Malware übernimmt die Berechtigungen des angemeldeten Benutzers. Im Falle eines Kontos mit administrativen Rechten können - im Normalfall geschützte - Dateien und Verzeichnisse modifiziert oder gelöscht werden. Weiterhin wird die Ausbreitung der Malware auf andere Systeme über das Netzwerk erleichtert.

Maßnahme: Benutzer, die ab und zu administrative Rechte benötigen, erhalten ein zweites Benutzerkonto mit dem sie Installationen oder administrative Tätigkeiten im Rahmen ihres Berechtigungsrahmens durchführen. Nach Beendigung der administrativen Tätigkeiten wird der Standardbenutzer für das normale Tagesgeschäft genutzt. Alle Standardbenutzerkonten werden auf die erforderlichen Berechtigungen reduziert.

[1] BSI Pressemitteilung vom 19.11.2015: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob=publicationFile&v=3

GCT Gesellschaft für Computer-Technologie mbH
Hausanschrift Im Atzelnest 3 · 61352 Bad Homburg
Telefon 06172 9486-0 · Telefax 06172 9486-94
Mail hallo@gct.de · Web www.gct.de
Twitter @GCT_BadHomburg · Facebook facebook.com/gct.it

Autor: Udo Janßen
Erstellt am: 10.12.2015
Revision am: 15.03.2016

Neue Gefahren aus dem Internet erfordern neue Maßnahmen

Zugriffsrechte auf Daten nach Bedarf für die zu erledigenden Tätigkeiten vergeben

Am Beispiel der „Crypto-Viren“ genannten Malwaregruppe kann die Sinnhaftigkeit einer gezielten Rechtevergabe erläutert werden. Wie im zuvor genannten Beispiel der Anmelderechte, kann durch Einschränkung der erforderlichen Rechte auf den tatsächlichen Bedarf für das tägliche Arbeiten eine Schadensbegrenzung bei Malwarebefall erzielt werden. Crypto-Viren nutzen Schwachstellen in Hilfsprogrammen, wie z.B. Adobe Flashplayer, Java, usw. beim Internetsurfen, sowie das unachtsame Ausführen von Programmen aus E-Mail Anhängen oder Downloadlinks.

Problem: Wird man Opfer einer solchen Attacke, durchsucht die Malware alle lokalen und Netzwerk-Laufwerke, auf die der angemeldete Benutzer Schreib- und Änderungsrechte hat. Findet die Malware dort mit Office erstellte Dateien (Word, Excel, usw.) - sowie je nach Ausprägung auch andere Dateitypen wie Bilder - verschlüsselt die Malware diese Dateien und hinterlässt zusätzlich einen „Erpresserbrief“. In diesem Erpresserbrief stehen Überweisungsdaten für Bitcoins[2] und eine variable Summe, um (vermeintlich) den Schlüssel zur Wiederherstellung und Entschlüsselung der Daten zu erhalten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie die Kriminalpolizei rät davon ab, auf die Forderungen einzugehen[3]. Es ist vorgekommen, dass nach Lösegeldzahlung kein Schlüssel übergeben wurde, oder nach Teilentschlüsselung eine erneute Forderung auf den Erpressten zukam. Nur das Wiederherstellen dieser Daten aus einem vorhandenen - nicht kompromittierten - Backup ist eine 100%ige Absicherung gegen den totalen Datenverlust. Die erforderlichen Nacharbeiten an Daten, die seit dem letzten Backup bearbeitet oder neu erstellt wurden, sind Schaden genug.

Maßnahme: Um den Schaden so gering wie möglich zu halten, organisiert man die Dateiablage granular nach den für die Zusammenarbeit erforderlichen Zugriffsrechten. Sollte ein Malwarebefall mit einem Crypto-Virus über einen Benutzer erfolgen, ist der Schaden zumindest auf die im Zugriff dieses Benutzers befindlichen Daten begrenzt.

Software auf Arbeitsplätzen automatisiert auf dem aktuellen Stand halten

Problem: Wie bereits zuvor erwähnt, sind Sicherheitslücken eines der häufigsten Einfallstore an Benutzersystemen. Sicherheitslücken ermöglichen der Schadsoftware - zum Teil ohne Benutzerinteraktion – die direkte Ausführung oder das Nachladen weiterer Schadsoftware. Durch das Aktualisieren der Anwendungssoftware und Hilfsprogramme auf den Benutzersystemen mit von den Herstellern bereitgestellten Sicherheitspatches, handelt man im Rahmen der möglichen Vorsorge verantwortungsvoll, ohne allerdings eine 100%ige Sicherheit zu erreichen. Jedoch erhält man dadurch mit vertretbarem Aufwand und Kosten einen weitreichenden Schutz.

Maßnahme: Einsetzen einer Softwarelösung zum automatisierten Patchen von Betriebssystemen und Anwendungsprogrammen.

[2] Digitale Geldeinheit, siehe https://de.wikipedia.org/wiki/Bitcoin
[3] http://www.polizei-praevention.de/themen-und-tipps/pc-gesperrt-ransomware.html

Neue Gefahren aus dem Internet erfordern neue Maßnahmen

GCT bietet mit dem Service **„careITclient“** eine Patchmanagement-Lösung für Clientcomputer (PC, Notebooks) an.

E-Mails mit Anlagen bieten den Malwareprogrammierern eine einfache und multiple Verbreitungsmöglichkeit Ihrer Schadprogramme

E-Mail ist eine einfach zu bedienende und im Geschäftsalltag unverzichtbare Kommunikationsplattform.

Problem: Mittels an das E-Mail angehängter Anlagen können Schadprogramme verteilt und ausgeführt werden. Sofern Virenscanner die Schadsoftware nicht erkennen und die Benutzerrechte weitreichend sind, steht der Ausbreitung der Malware nichts mehr im Wege. Grundsätzlich ist das Verteilen von Informationen per E-Mail unter Einhaltung von akzeptablen Anlagengrößen[4] verbreitet und auch akzeptiert. Handelt es sich jedoch um potentiell gefährliche und ausführbare Dateien, sollte man von der Verteilung per E-Mail absehen und auch den Empfang solcher Mailanlagen am Mailgateway des Unternehmens unterbinden.

Durch das automatische Blocken von ausführbaren Dateien, die als Mailanlagen empfangen werden, wird das Sicherheitsniveau enorm erhöht und das versehentliche Ausführen von Schadsoftware eingedämmt. Unterbindet man zusätzlich das Versenden dieser ausführbaren Dateien, verhindert man, dass man selbst zum unfreiwilligen Verteiler von Schadprogrammen wird.

Eine Renaissance erlebt derzeit (Anfang 2016) auch die Gruppe der Macroviren. Mit „Locky“ wird eine ausgeklügelte Ransomware[5] Variante über Macroviren (Word-, Excel Dokumente) vornehmlich über E-Mail verbreitet. Abhängig von den Sicherheitseinstellungen im jeweiligen Office Programm wird direkt beim Öffnen der Datei der Macrovirus aktiv. Sollte eine Bestätigung zur Ausführung von Macros konfiguriert sein, und der Benutzer diese Bestätigung erteilen, wird der Macrovirus dann ausgeführt. Im Hintergrund wird ein Download gestartet. Dadurch sind die Entwickler des Macrovirus auch in der Lage, Anpassungen auf Ihren Quellen durchzuführen und den Virus so zu „optimieren“. Das heruntergeladene Programm wird dann mit den Rechten des Benutzers ausgeführt und verschlüsselt die für den Benutzer mit Schreibrecht versehenen Dateien. Hinterlassen wird zusätzlich eine Datei mit dem „Erpresserbrief“, der zur Zahlung von Lösegeld auffordert, um die Daten wieder zu entschlüsseln (siehe Kapitel „Zugriffsrechte auf Daten nach Bedarf für die zu erledigenden Tätigkeiten vergeben“).

Maßnahme: Verhindern des Empfangs - also vor Eintreffen im Postfach des Empfängers - und Versands von ausführbaren Dateien am Mailgateway. Es bestehen Möglichkeiten, entweder den Absender in einer automatisierten Systemnachricht über die abgelehnte Mail zu informieren oder die Mail in einem internen Quarantänebereich abzulegen. Dieser Quarantänebereich muss dann jedoch von geschultem Personal gesichtet und bearbeitet werden. Wir empfehlen das konsequente Ablehnen von ausführbaren Dateien und Information des Absenders in einer automatisierten Systemnachricht. Stellen Sie Ihre sensiblen Daten stattdessen über eine geschützte Austauschplattform zur Verfügung.

Um den Schutz bzgl. Microsoft Office Dokumenten mit eingebetteten Macros zu erhöhen, sind umfassendere Maßnahmen erforderlich. Unternehmen verzichten ungern auf die Möglichkeit des E-Mail

[4] Auch wenn im Mailstandard keine definierte Grenze der Anlagengrößen vorhanden ist, begrenzen Mailserver-Betreiber die Größen von Emails um Systemüberlastungen zu vermeiden. Wir empfehlen Mailgrößen auf 20MB zu limitieren.
[5] BSI Definition von Ransomware: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf

Neue Gefahren aus dem Internet erfordern neue Maßnahmen

Empfangs und Versands von Office Dokumenten. Der Verweis, man könne ja auf PDF-Dokumente ausweichen, verlagert nur die Gefahr von Office auf PDF. PDF Dokumente besitzen ebenso häufige und ähnliche Sicherheitsrisiken.

Über MS Office Gruppenrichtlinien (Voreinstellungen der Sicherheitseinstellungen) kann man ein gutes Maß an Sicherheit erreichen, wenn man bereit ist, organisatorische Maßnahmen in seinem Unternehmen umzusetzen. Ist man dazu nicht bereit, muss man dieses Risiko akzeptieren.

Eine ideale, sichere und trotzdem einfach zu bedienende Dateiaustauschplattform bietet die „GCT hostITbox“. Dort können Dateien - angekündigt und wenn gewünscht vertraulich authentifiziert – sicher ausgetauscht werden. Die geschäftlichen Daten liegen während des Austauschs im Rechenzentrum der GCT (Frankfurt am Main) und nicht auf irgendwelchen Servern irgendwo in der Welt (Stichwort: Dropbox, u.a.).

Eingebettete Links in E-Mails oder Links auf Webseiten und Suchmaschinen ermöglichen Schadsoftwareverteilern eine einfache Möglichkeit, ihre Programme in Unternehmensnetzwerken zur Ausführung zu bringen

Seit geraumer Zeit (Stichwort: ***Snowden***) ändern Webseitenbetreiber den Zugang zu Ihren Webseiten auf verschlüsselte Verbindungen. Wohl prominentestes Beispiel ist Google. Beim Zugriff auf http://www.google.de wird automatisch auf https://www.google.de verwiesen, für den Aufrufer der Website transparent und kaum erkennbar[6].

Problem: Grundsätzlich ist dieses Vorgehen sehr positiv zu bewerten, da dadurch das „Mitlesen“ der übertragenen Daten durch unbefugte Dritte verhindert wird. Leider verhält sich das aber für die vom Unternehmen eingesetzten Sicherheitssysteme genauso: Eine im Datenstrom stehende Firewall mit Malwareschutz ist „blind“ für verschlüsselte Kommunikation und kann diese nicht auf gefährliche Inhalte untersuchen. Das bietet für Malwareverteiler ein Schlupfloch, um unerkannt Schadsoftware ins Unternehmensnetz einzuschleusen. Dieser Praxis begegnet man von Unternehmensseite mit dem Aufbrechen der verschlüsselten Kommunikation am Gateway, damit das Firewall System gefährliche Inhalte erkennen und unterbinden kann. Mitarbeiter müssen dabei beachten, dass private Kommunikation und private Aufrufe von Webseiten auch von dieser Art der Prüfung betroffen sind. Ist man persönlich nicht mit der Untersuchung einverstanden, unterlässt man das Surfen während der Arbeitszeit und führt das in seinem privaten Netzwerk zu Hause oder über Mobilfunk durch.

[6] je nach Browser durch ein schlossartiges Symbol und ggf. eine grün eingefärbte Webadressen-Leiste

Neue Gefahren aus dem Internet erfordern neue Maßnahmen

Maßnahme: Einsatz eines Firewall Gateways mit SSL Inspektionstechnik. Wie oben beschrieben, erkennt das Firewall System mit aktiviertem DPI-SSL für Clients den Aufruf von verschlüsselten Verbindungen und bringt sich in den Datenstrom ein. Indem ein von der Firewall ausgestelltes Zertifikat für die interne Verbindung benutzt wird, kann die Firewall den Datenstrom untersuchen und baut von sich aus eine erneute verschlüsselte Verbindung zum eigentlichen Zielserver auf. Daher ist die Verbindung über das Internet gesichert und nur auf dem Firewall System erfolgt eine Untersuchung des Datenstroms auf gefährliche Inhalte (Antivirus, Intrusion Prevention, Anti Spyware, Content Filter – abhängig von den lizenzierten Services).

GCT setzt bei seinen Kunden SonicWALL Firewall Systeme mit DPI-SSL (Deep Packet Inspection für SSL) ein.

Udo Janßen ist seit 1990 bei GCT und seit 2001 als geschäftsführender Gesellschafter für die Technik verantwortlich. Er hat bei zahlreichen Unternehmen aus dem KMU-Segment Netzwerk- und Securityinfrastrukturen aufgebaut und ist von Herstellern wie u.a. SonicWALL, Microsoft, VMware, Kemp als Administrator zertifiziert.

GCT ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.