TODO-Liste IT-Sicherheit:

Technische Maßnahmen zur Absicherung der Domain Controller:

- ☐ Einsatz von Application Whitelisting (z.B. Microsoft Applocker) auf allen Domain Controllern (später auch auf allen Windows Servern)
- ☐ Einsatz einer Host Based Firewall (z.B. Microsoft Firewall) auf allen Domain Controllern mit einem möglichst harten Regelwerk (später auch auf allen Windows Servern)
- ☐ Intensives Logging auf den Domain Controllern (z.B. gemäß Corporate Trust Logeinstellungen)
- ☐ Reduktion der Personen mit Domain Admin Berechtigungen auf möglichst wenig Accounts (need to know Prinzip). Optional: Einsetzen einer Software zum Management von administrativen Aktionen[1] oder tokenbasierte Authentifizierung[2] für Admins.
- ☐ Trennung der Domain Admin Accounts von den normalen Admin Accounts (ein Domänenadministrator hat damit drei Accounts: seinen User-Account, seinen Admin-Account und seinen Domain-Admin Account, letzterer sollte nur möglichst spärlich genutzt werden).
- ☐ Verwaltung der Domain Controllern nur per RDP over IPSEC von dedizierten, hochgesicherten Bastion Hosts (d.h. die Domain-Admin Accounts werden nie auf unsicheren Maschinen verwendet)
- ☐ Aufstufen des Domain Feature Level auf mindestens 2007, Nutzung aller Sicherheitsfunktionen. D.h. vor allem, dass Sie eine eigene Passwort Policy für Admin Accounts vergeben können und für diese Accounts ein mindestens 12-stelliges Passwort verlangen können.
- ☐ Zur Minimierung der Angriffsfläche: Auf allen Servern und Clients: Abschaffung möglichst aller lokalen Administrator Accounts und rasches Einspielen von Updates und Sicherheitspatches.
- ☐ Strikte Einhaltung der Microsoft Empfehlungen bzgl. Domänensicherheit

Strategisch: Konzentration auf ein verteidigbares Netzwerk:

- ☐ Homogenisierung der verwendeten IT-Komponenten, konsequentes Abschalten veralteter Hardware bzw. Software.
- ☐ Erweiterung des heute meist dreistufigen Netzwerks (Internet - DMZ - Intranet) auf mindestens 6-8 Sicherheitszonen.
- ☐ Entwicklung einer Log Policy und überprüfen ob die Logeinstellungen an allen Servern und Clients stimmen, Einführung einer Logkonsolidierung wie z.B. Splunk.

Organisatorisch: 100% Sicherheit gibt es nicht. Jede Firma muss sich auf einen Ernstfall vorbereiten:

- ☐ Generell gilt: solange das Ausmaß des Angriffs noch nicht bekannt ist, sind Abwehrmaßnahmen reine Glückssache und selten sinnvoll und zielgerichtet einsetzbar. Daher: Kontakt mit einem geeigneten Dienstleister (z.B. Corporate Trust) herstellen und ggf. dessen schnelle Verfügbarkeit über eine Krisenhotline sicherstellen. Alternativ: Verfügbarkeit über eine Cyber-Versicherung herstellen.
- ☐ Rein technische Gegenmaßnahmen helfen in der Detektion, reduzieren Schaden und minimieren Angriffsmöglichkeiten - verhindern aber keine Industriespionage und beenden keinen laufenden Angriff. Einem gezielt vorgetragenen Angriff muss man ein mit gutem Know How ausgestattetes Verteidigungsteam entgegenstellen, welches die technischen Sicherheitsmaßnahmen ergänzt / flankiert.
- ☐ Die Angreifer wählen die Waffen, Zeitpunkt und Schlachtfeld: d.h. sie haben freie Wahl mit welchen Tools sie wann welchen Server angreifen und haben damit einen Vorteil gegenüber der Verteidigung. Die Vorteile des Verteidigungsteams sind die bessere Kenntnis der Infrastruktur und die weitreichenderen Handlungsmöglichkeiten in der internen IT. Dazu benötigt das Verteidigungsteam ausreichende Kompetenzen damit das Team auch wirklich bessere Handlungsmöglichkeiten als die Angreifer hat.

[1] Z.B. mittels http://www.cyberark.com/
[2] https://de.wikipedia.org/wiki/Einmalkennwort

Begründung dieser Maßnahmen am Beispiel des Cyberangriffs auf den Bundstag

11.06.2015 – Nach Recherchen von NDR, WDR und "SZ" sagen Experten des Bundesamtes für Sicherheit in der Informationstechnik, das Netzwerk des Bundestags sei nach der schweren Hackerattacke die Mitte Mai 2015 entdeckt wurde nicht mehr zu retten. Es wird von einem „Totalschaden", einer „Aufgabe des Netzwerks", einem notwendigen Hardwaretausch und einer kompletten Neuinstallation gesprochen. Die Corporate Trust ist nicht in diesen Fall involviert – allerdings kennen wir die in der Presse beschriebenen Symptome aus etlichen unserer aktuellen Fälle. Daher können wir in dieser Presse- und Kundeninformation einige Hintergrundinformationen liefern.

Voraussetzung für einen erfolgreichen Angriff ist immer die Infiltration des Zielnetzwerks. Dies wird in der Regel mit einer gezielt für das Opfer vorbereiteten, bösartigen E-Mail gemacht (sogenanntes Spear-Phishing[3]) die dann einen Trojaner einschleust. Angesichts der Tatsache, dass wir in der IT den Kampf gegen die Malware (Viren und Trojaner) gerade generell verlieren[4] steigt das Risiko für jede Organisation an, Opfer einer solchen Attacke zu werden.

Ist ein Trojaner einmal eingeschleust, wird versucht, an ein möglichst hochwertiges Passwort heranzukommen. Das Ziel ist typischerweise das Passwort eines IT-Administrators. Erster Schritt dazu ist es, die Kontrolle über den infizierten Rechner zu bekommen (im Fachjargon: lokale Administratorrechte). Generell gilt: je älter das System ist, desto leichter ist das. Auch die Konfiguration im Unternehmen und die Aktualität der eingespielten Updates spielt hierbei eine Rolle. Im Regelfall wird ein Angreifer in vielen Netzwerken aber sehr oft noch auf veraltete Systeme treffen (teilweise Windows XP), die ihm die Arbeit hier stark erleichtern. Oft haben in Firmen auch viele oder alle Mitarbeiter diese Rechte ohnehin – dann muss ein Angreifer hier keine weitere Zeit verschwenden.

Danach wird typischerweise eine Angriffstechnik verwendet, die sich Pass-the-Hash (PtH) nennt. Wenn ein Nutzer sich mit seinem Passwort unter Windows anmeldet, dann wird eine nicht wiederherstellbare Form dieses Passwort zwischengespeichert (diese Form nennt man Hash). Dieser Hash wird benutzt, um im Hintergrund die Anmeldung an weitere Computer weiterzureichen, damit der Benutzer das Passwort nicht ständig neu eingeben muss. Besitzt ein Angreifer lokale Administratorrechte, kann er diese Hashes verwenden um sich an weiteren Systemen anzumelden und sich dort weitere Hashes zu holen[5]. Dies wiederholt der Angreifer solange, bis er die Berechtigung eines hohen IT-Administrators erlangen konnte. Eine solche PtH-Attacke ist eine spezielle Form des Logindaten-Diebstahls, und sie lässt sich nicht verhindern – d.h. Ziel ist es, dem Angreifer das Erlangen der Voraussetzung für diese Attacke (die Administratorberechtigung) möglichst schwer zu machen.

Alle Windows PCs sind in einem Microsoft Netzwerk zusammengefasst, das sich Domäne nennt und durch mehrere spezielle Rechner (sogenannte Domain Controller) verwaltet wird. Innerhalb der Domäne werden alle Benutzerberechtigungen mit einem Kerberos genannten System verwaltet. Wenn ein Benutzer eine Anwendung im Netzwerk nutzen will, so holt er sich beim Domain Controller ein sogenanntes Kerberosticket, welches er dann bei der Anwendung die er nutzen will vorzeigt. Dieser Prozess läuft im Hintergrund in jeder Firma der Welt tausendfach ab. Auch Sie haben sich heute sicherlich schon ein Kerberosticket besorgt. Ein Kerberosticket hat typischerweise eine Laufzeit von einigen wenigen

[3] https://de.wikipedia.org/wiki/Phishing
[4] http://www.av-test.org/de/statistiken/
[5] https://www.sans.org/reading-room/whitepapers/testing/passthehash-attacks-tools-and-mitigation-33283

Stunden (je nach Konfiguration 2-12h), danach ist eine Neuausstellung bzw. eine Neuanmeldung notwendig.

Ziel des Angreifers ist nun die Berechtigung eines sogenannten Domänen-Administrators. Mit dieser Berechtigung kann sich ein Angreifer dann mit einem Hackertool namens mimikatz ein sogenanntes „Golden Ticket“ erstellen[6]. Ein solches Ticket nutzen z.B. auch die Domain Controller um sich gegenseitig die vollen Berechtigungen für eine lange Laufzeit (10 Jahre) zu geben. Stellen Sie sich vor, sie hätten einen Schlüssel für jedes Haus und jede Wohnung in Ihrer Stadt. Und das tollste ist, wenn Sie diesen Schlüssel benutzen, dann verwandeln Sie sich gleichzeitig automatisch in den Hausbesitzer. Ein Angreifer der ein Golden Ticket besitzt, hat etwa analoge Fähigkeiten in Ihrem Netzwerk.

Der nächste Schritt des Angreifers ist nun einfach: ausgestattet mit den höchstmöglichen Berechtigungen geht es nun darum, geheime Zugangspunkte an möglichst vielen Stellen im Netzwerk zu verstecken. Das können SmartTVs in Besprechungsräumen, PCs in Robotersteuerungen, der Vorstands-PC, der Hauptrouter im Netzwerk, das Voice-over-IP Telefon des Entwicklungsleiters und jegliche andere Computertechnologie sein. Um die Sache ein bisschen komplizierter zu machen, kann sich ein Angreifer auch so tief in Hardware eingraben, dass eine Bereinigung durch eine Softwareneuinstallation nicht mehr in einem sinnvollen Kostenrahmen möglich ist und die Hardware ausgetauscht werden muss. Ein bekannter Vorfall ist z.B. die Schadsoftware der „Equation Group“ die unter anderem die Fähigkeit besitzt, die Festplatten-Firmware verschiedener Hersteller darunter Seagate, Western Digital, Toshiba, Maxtor und IBM umzuschreiben[7]. Es gibt aber bereits Hinweise, dass diese Angriffsmöglichkeit auch für die Software der Computerhauptplatine (das BIOS) bzw. für Netzwerkkarten denkbar ist[8].

Hat ein Angreifer erstmal ein Golden Ticket erhalten und konnte mit diesem ein paar Stunden „spielen gehen“, dann ist die Aussage, dass das Netzwerk verloren ist, nicht übertrieben. Allein um das Golden Ticken zu widerrufen ist eine komplexe Nachsicherungoperation[9] notwendig. Um aber alle Folgen einer solchen Infektion sicher zu beseitigen müssen wohl alle Rechner neuinstalliert und ggf. auch die komplette Hardware ausgetauscht werden. Dies ist nicht möglich wenn der Hacker zeitgleich noch an anderen Stellen im Netzwerk ist, d.h. für die Bereinigung muss entweder das gesamte Netz vom Internet getrennt oder alle Computer abgeschaltet werden. Dies ist normalerweise nicht möglich ohne die Existenz einer Firma zu gefährden. Im Bundestag besteht durch die Sommerpause im August eventuell sogar eine realistische Chance für eine solche Nachsicherung. Im Normalfall wird eine Firma ein so kompromittiertes Netz als „unsicheres Intranet“ weiterbetreiben und mit einer neuen sicheren Keimzelle beginnend ein neues „Netzwerk im Netzwerk“ aufbauen. Zuerst werden in diesem neuen Netzwerk nur die sensibelsten Daten verarbeitet später übernimmt es sukzessive die Aufgaben des alten Netzwerks. Dieser Prozess kann sich über mehrere Jahre ziehen, während derer man sich mit den Hackern im alten, unsicheren Netzwerk ein Rückzugsgefecht liefert um ihnen den weiteren Datenabfluss wenigstens so schwer wie möglich zu machen.

[6] http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf
[7] https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/
[8] https://deepsec.net/docs/Slides/2014/A_Myth_or_Reality___BIOS-based_Hypervisor_Threat_-_Mikhail_Utin.pdf
https://www.blackhat.com/presentations/bh-usa-09/WOJTCZUK/BHUSA09-Wojtczuk-AtkIntelBios-SLIDES.pdf
https://conference.hitb.org/hitbsecconf2014kul/materials/D1T1%20-%20SENTER%20Sandman%20-%20Using%20Intel%20TXT%20to%20Attack%20BIOSes.pdf
[9] https://technet.microsoft.com/en-us/library/bb727066.aspx?f=255&MSPPError=-2147217396#ECAA