Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

SICHERER KOMMUNALER IT-ARBEITSPLATZ

IT-Sicherheitsempfehlungen zum Betrieb von Fachverfahren

SICHERER KOMMUNALER IT-ARBEITSPLATZ

IT-Sicherheitsempfehlungen zum Betrieb von Fachverfahren

Dr. Steven Arzt

Dr. Philipp Holzinger

Fraunhofer-Institut für Sichere Informationstechnologie, SIT
Rheinstraße 75
64295 Darmstadt

Projektpartner: AKDB

Version vom 09.10.2020

Inhalt

1 Einführung 5
1.1 Management Summary 5
1.2 Zielgruppe 5
1.3 Systembeschreibung 6

2 Risikobetrachtung 7
2.1 Assets 7
2.1.1 Primäres Asset 7
2.1.2 Sekundäre Assets 7
2.2 Angreifer 8
2.3 Angriffsziele 9
2.4 Angriffswege 9
2.4.1 A1: Kompromittieren des Client-PCs 9
2.4.2 A2: Kompromittieren des Datenbankservers 9
2.4.3 A3: Kompromittieren der Datenübertragung zwischen Client und Server 10
2.4.4 A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren 10
2.4.5 A5: Manipulation des Fachverfahrens auf dem Client-PC 10

3 Netzwerksicherheit 11
3.1 Client-Authentifizierung 11
3.2 VPN 12
3.3 Perimeter-Firewall 13
3.4 Host-basierte Firewall 14
3.5 Isolation virtueller Teilnetze 14
3.6 Isolation des Datenbankservers 15
3.7 Verschlüsselung der Netzwerkkommunikation 15
3.8 Physische Zugriffskontrolle für Netzwerk 16

4 Hostsicherheit 18
4.1 Logische Zugriffskontrolle für PCs und Server 18
4.2 Passwortrichtlinien 19
4.3 Planmäßige Softwareupdateprozesse 20
4.4 Einschränkung der Benutzerrechte am Client-PC 21
4.5 Automatisches Sperren 22
4.6 Malware-Erkennung auf Hostsystem 23
4.7 Datenträgerverschlüsselung 23
4.8 Schutz von Browser und Mailclient 24
4.9 Einsatz eines Terminalservers 25
4.10 Automatische Datensicherung 26
4.11 Secure Boot 26
4.12 Physische Zugriffskontrolle für PCs und Server 27
4.13 Bildschirmschutz 27
4.14 Physischer Schutz von Hardwareschnittstellen 28

5 Organisatorische Maßnahmen 29
5.1 Eingeschränkte Softwareauswahl für PCs und Server 29
5.2 Security-Awareness-Training für Mitarbeiter 29
5.3 Externe Dritte nicht unbeobachtet mit Hardware lassen 30

6 Abschluss 31

1 Einführung

1.1 Management Summary

Die AKDB entwickelt verschiedene Fachverfahren für den Einsatz in Behörden und Kommunen. Die jeweiligen Betreiber sind in der Verantwortung für die Einrichtung und den Betrieb einer IT-Infrastruktur, die den sicheren Einsatz der AKDB-Fachverfahren unterstützt.

Das vorliegende Dokument soll wichtige Sicherheitsaspekte und Maßnahmen beleuchten, die dem sicheren Betrieb von Fachverfahren zuträglich sein können. Die Maßnahmen sind nicht nur spezifisch für AKDB-Fachverfahren anwendbar, sondern gelten ebenso für Anwendungen mit ähnlichem Architektur- und Sicherheitskonzept.
Besonderes Augenmerk gilt hier dem Betrieb von Fachverfahren in einer sogenannten „2-Tier-Architektur“ (wesentliche Systemmerkmale siehe Abschnitt 1.3); viele der dargestellten Maßnahmen sind aber auch generell sinnvoll.

Hierbei handelt es sich um allgemeine Empfehlungen, die jedoch stets anhand der Gegebenheiten und Anforderungen der jeweiligen Betreiber geprüft und angepasst werden müssen. Allgemeine Sicherheitsempfehlungen, die sich für den Betreiber aus Compliance-Anforderungen (z.B. EgovG des Bundes und der Länder, DSGVO, SGB, AO, BMG, etc.) oder anderen Gründen ergeben, sollen nicht ersetzt werden. Stattdessen sollen hier zusätzliche Hinweise gegeben werden, deren Berücksichtigung zu einem sicheren IT-Arbeitsplatz insgesamt beitragen kann.

Im Hauptteil des Dokuments folgen nach einer Risikobetrachtung (Kapitel 2) technische Empfehlungen zur Netzwerksicherheit und Sicherheit der Rechnersysteme (Kapitel 3 und 4); die Auswahl der aufgeführten Maßnahmen und die zusätzliche Priorisierung am jeweiligen Kapitelanfang basiert auf der Sicherheitsexpertise der Autoren und dem besonderen Fokus auf Fachverfahren, deren Architektur der Beschreibung in Abschnitt 1.3 gleicht. Es folgen wichtige organisatorische Maßnahmen (Kapitel 5). Den Abschluss (Kapitel 6) bildet nochmals der besondere Hinweis auf die Verantwortung des jeweiligen Betreibers.

1.2 Zielgruppe

Behörde und Kommune als Betreiber eines Fachverfahrens

- Administratoren
- „Power-User“
- Sicherheitsverantwortliche
- Management / Entscheider

1.3 Systembeschreibung

Für den Betrieb eines Fachverfahrens wird ein – zumeist von Microsoft-Systemprodukten geprägter – Systemkontext angenommen, der aus mehreren Teilsystemen besteht:

- **Client-PC**
  Auf dem Client-PC sind die Programmdateien des Fachverfahrens installiert und dort werden sie ausgeführt. Das Fachverfahren greift vom Client-PC direkt auf den Datenbankserver zu, um Daten zu lesen und zu schreiben.
- **Datenbankserver**
  Der Datenbankserver speichert die Daten, die vom Fachverfahren auf dem Client-PC erfasst, angezeigt und bearbeitet werden. Client-PCs und Datenbankserver tauschen Daten über eine lokale Netzwerkverbindung aus. Hierfür verwendet das Fachverfahren ein allgemeines Benutzerkonto für die Authentifizierung am Datenbankserver, das von allen Instanzen des Fachverfahrens, unabhängig vom jeweiligen Nutzer, auf allen Client-PCs des jeweiligen Betreibers verwendet wird. Die feingranulare Zugriffskontrolle auf einzelne Datensätze der Datenbank entsprechend der Benutzerrechte des angemeldeten Nutzers erfolgt also ausschließlich im Fachverfahren auf dem Client-PC und nicht auf dem Datenbankserver, woraus sich zusätzliche Angriffsmöglichkeiten ergeben.
- **Domain-Controller mit DHCP und DNS**
  Der Domain-Controller dient dem Betrieb von Active Directory, was zum Management von Clients und Servern, und u. a. zur Verwaltung von Benutzern und Rechten, verwendet wird.
- **Mailserver**

Es wird im Folgenden die Annahme getroffen, dass sich alle Systeme lokal vor Ort in den Räumlichkeiten des Betreibers befinden.

2 Risikobetrachtung

Die Risikobetrachtung in diesem Kapitel erfolgt auf Grundlage der Eigenschaften von 2-Tier-Fachverfahren (Systembeschreibung siehe Abschnitt 1.3), wie zum Beispiel das im Kontext dieses Dokuments näher betrachtete AKDB-Fachverfahren OK.FIS[1]. Die nachfolgenden Darstellungen sind jedoch übertragbar auf andere Fachverfahren, die ein ähnliches Architektur- und Sicherheitskonzept implementieren.

2.1 Assets

Assets repräsentieren die schützenswerten Güter des Systems. Primäre Assets sind hierbei die eigentlichen Werte, die es zu schützen gilt. Sekundäre Assets können sich aus technischen Gegebenheiten oder Sicherheitsmaßnahmen ergeben, die letztlich dem Schutz der primären Assets dienen. *Beispiel: Im Rahmen einer Datenverschlüsselung entsprechen die zu verschlüsselnden Daten dem primären Asset, wohingegen der kryptographische Schlüssel ein sekundäres Asset darstellt – der Schlüssel ist nur von Relevanz, weil er Zugriff auf die ursprünglichen Daten ermöglicht.*

Der hier betrachtete Kontext umfasst das Fachverfahren selbst, sowie die Daten und Systeme, die für den Betrieb notwendig sind. Hieraus ergeben sich die im Folgenden aufgeführten Assets.

2.1.1 Primäres Asset

- **Daten in der Datenbank**
  Können personenbezogene oder anderweitig sensitive Daten sein, deren Vertraulichkeit und Integrität von großer Wichtigkeit ist.
  Manifestationen:
  - Datenbankserver (Festspeicher, Arbeitsspeicher)
  - Client-PC (Festspeicher, Arbeitsspeicher, Bildschirm)
  - Netzwerkübertragung zwischen Datenbankserver und Client-PC (unverschlüsselt & unauthentifiziert)

2.1.2 Sekundäre Assets

- **Zugangsdaten der Benutzer für das Fachverfahren**
  Sie können vom Sachbearbeiter gleichermaßen wie vom Angreifer benutzt werden, um auf Datenbankinhalte zuzugreifen.
- **Programmordner des Fachverfahrens auf dem Client-PC**
  Im Fall des hier näher betrachteten Fachverfahrens und möglicherweise anderer Fachverfahren beinhaltet der Programmordner, gegebenenfalls obfuskiert, Zugangsdaten zur Datenbank, sowie ausführbare Programmdateien, in welche der Sachbearbeiter seine Zugangsdaten

[1] Softwareprodukt für die Finanzverwaltung einer Kommune

eingibt, und die eine clientseitige Zugriffsprüfung auf Datenbankinhalte durchführen.

- **Installationsdateien des Fachverfahrens**
  Beinhaltet den Programmordner, der im Fall des hier betrachteten Fachverfahrens und möglicherweise anderer Fachverfahren Zugangsdaten zur Datenbank beinhaltet.
- **Netzwerkinfrastruktur**
  Im Fall des hier betrachteten Fachverfahrens und möglicherweise anderer Fachverfahren wird der Datenbankinhalt behördenintern unverschlüsselt zwischen Client-PC und Datenbankserver über das Netzwerk übertragen.
- **Datenbankserverhardware**
  Die Hardware beinhaltet Repräsentationen des Datenbankinhalts im Fest- und Arbeitsspeicher. Die Manipulation der Hardware kann das Verhalten des Systems zugunsten des Angreifers verändern.
- **Client-PC-Hardware**
  Die Hardware beinhaltet Repräsentationen des Datenbankinhalts im Fest- und Arbeitsspeicher. Die Manipulation der Hardware kann das Verhalten des Systems zugunsten des Angreifers verändern.
- **Client-PC Systemsoftware und Konfiguration**
  Durch Manipulation der Software, oder das Ausnutzen von Schwächen in der Systemsoftware oder –konfiguration kann der Angreifer logischen Zugriff erlangen
- **Client-PC-Bildschirminhalt**
  Der Inhalt der Datenbank wird zeitweise auf dem Bildschirm dargestellt
- **Gruppenrichtlinie**
  Die Gruppenrichtlinie regelt den Zugriff auf den Client-PC, sowie den Datenbankserver. Durch Manipulation könnte der Angreifer Zugriff erhalten oder seine Rechte erweitern.

Alle in den Kapiteln 3-5 betrachteten Maßnahmen dienen letztlich dem Schutz der Daten in der Datenbank vor Manipulation und unbefugtem Zugriff.

2.2 Angreifer

Bezug zur Organisation:

- **Externe Angreifer**
  - Kein Mitarbeiter und Dienstleister des Betreibers
- **Interne Angreifer**
  - Mitarbeiter oder Dienstleister des Betreibers

Bezug zur Örtlichkeit:

- **Entfernter Angriff**
  - Der Angreifer ist in geographischer Distanz und interagiert mit Zielsystemen und Zielpersonen z.B. per Internet, Telefon oder Post
- **Lokaler Angriff**
  - Der Angreifer ist lokal beim Betreiber vor Ort und hat physischen Zugriff auf Zielsysteme und Zielpersonen

Das Hauptaugenmerk liegt auf externen Angreifern, die entfernte Angriffe durchführen. Derartige Angriffe sind in der Praxis besonders häufig zu erwarten, unter anderem, da sie in der Regel mit geringem Ressourcenaufwand durchführbar

sind und daher gut skalieren. Die nachfolgende Empfehlung von Sicherheitsmaßnamen berücksichtigt jedoch auch andere Kategorien von Angriffen.

2.3 Angriffsziele

- **Unerlaubter Lesezugriff auf Datenbankinhalte**
- **Unerlaubter Schreibzugriff auf Datenbankinhalte**
- **Einschränkung der Erreichbarkeit der Datenbankinhalte**

2.4 Angriffswege

2.4.1 A1: Kompromittieren des Client-PCs

- **A1.1: Social Engineering**
  Beispiel: Der Angreifer kann einen Mitarbeiter veranlassen, Zugangsdaten preiszugeben, oder Schadsoftware zu installieren (z.B. durch Zusenden eines mit Schadcode hinterlegten Links in einer entsprechend glaubwürdig formulierten E-Mail)
- **A1.2: Physischer Zugriff auf die Festplatte**
  Beispiel: Der Angreifer kann Daten von der Festplatte kopieren, Schadsoftware installieren, oder darauf befindliche Programme und Konfigurationen manipulieren.
- **A1.3: Physischer Zugriff auf Eingabegeräte**
  Beispiel: Der Angreifer kann Manipulationen vornehmen, um Tastatureingaben mitzuhören.
- **A1.4: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber (z.B. USB)**
  Beispiel: Der Angreifer kann durch Einstecken bestimmter Hardware Schwachstellen im Treiber oder Betriebssystemkernel ausnutzen, um logischen Zugriff zu erlangen und Schadsoftware zu installieren.
- **A1.5: Ausnutzen einer Schwachstelle im Betriebssystem oder Anwendungssoftware**
  Beispiel: Der Angreifer kann eine Sicherheitslücke im Mail-Client ausnutzen, um Schadsoftware zur Ausführung zu bringen, ohne dass hierfür eine Benutzerinteraktion nötig wäre.
- **A1.6: Abfotografieren des Bildschirminhalts**
  Beispiel: Der Angreifer kann vor Ort mit einem Smartphone den Bildschirm eines Sachbearbeiters abfotografieren.
- **A1.7: Manipulation der Gruppenrichtlinie auf dem Domaincontroller**
  Beispiel: Der Angreifer fügt einen zusätzlichen Benutzer hinzu, der über administrative Rechte auf dem Client-PC verfügt.

2.4.2 A2: Kompromittieren des Datenbankservers

- **A2.1: Social Engineering**
- **A2.2: Ausnutzen einer Schwachstelle im Betriebssystem oder Dienstsoftware**
- **A2.3: Manipulation der Gruppenrichtlinie auf dem Domaincontroller**
- **A2.4: Physischer Zugriff auf die Festplatte**

- **A2.5: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber**

Siehe oben für Beispiele

2.4.3
A3: Kompromittieren der Datenübertragung zwischen Client und Server

- **A3.1: Physischer Zugriff auf die Datenübertragung**
  Der Angreifer könnte sich vor Ort Zugang zur Netzwerkinfrastruktur beschaffen, falls diese nicht ausreichend vor physischem Zugriff geschützt sein sollte. Dies könnte ein kabelgebundenes Netzwerk betreffen (LAN), sowie Funknetzwerke (WLAN).
- **A3.2: Logischer Zugriff auf die Datenübertragung**
  Unter Umständen könnte der Angreifer logischen Zugang zur Datenübertragung erlangen, wenn er Netzwerkhardware (Switch, Firewall, Router, etc.) kompromittiert, oder andere Systeme, die im gleichen Netzwerk sind und über Möglichkeiten verfügen, Netzwerkverkehr mitzuhören.

Die Kompromittierung der Datenbankübertragung gefährdet die Vertraulichkeit, Integrität und Authentizität der Datenbankinhalte, da die Verbindung zwischen Client-PC und Datenbankserver im Klartext erfolgt.

2.4.4
A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren

Im Fall des hier betrachteten Fachverfahrens und möglicherweise anderer Fachverfahren befinden sich die Zugangsdaten zu den Datenbankinhalten mit vollen Lese- und Schreibrechten, gegebenenfalls obfuskiert, in den Programmdateien, bzw. der Konfiguration des Fachverfahrens. Der Zugriff auf das Programmverzeichnis, oder auf die Installationsdateien kann daher von einem versierten Angreifer ausgenutzt werden, um diese Zugangsdaten zu rekonstruieren. Wir treffen hier die Annahme, dass die Programmdateien lokal auf dem Client-PC installiert sind. Dieser Angriff ist nicht relevant für Fachverfahren, die keine Zugangsdaten im Programmverzeichnis ablegen.

2.4.5
A5: Manipulation des Fachverfahrens auf dem Client-PC

Im Fall des hier betrachteten Fachverfahrens und möglicherweise anderer Fachverfahren führt das Fachverfahren selbst die Zugangskontrolle auf ausgewählte Datenbankinhalte clientseitig durch und blendet beispielsweise Daten aus, auf die der jeweils angemeldete Sachbearbeiter keinen Zugriff haben soll. Manipuliert der Angreifer das Fachverfahren und damit die Zugangskontrolle, kann die Zugangsbeschränkung aufgehoben werden. Dieser Angriff ist nicht relevant für Fachverfahren, die ausschließlich serverseitig Zugangskontrollen durchführen.

3 Netzwerksicherheit

Auf Basis der Risikobewertung werden im folgenden empfehlenswerte Maßnahmen zur Netzwerksicherheit vorgestellt.

Die Grundannahme ist, dass Client-PCs, die das Fachverfahren ausführen, sowie weitere, für den Betrieb notwendige Systeme sich in einem lokalen Netzwerk beim Betreiber vor Ort befinden. Der Zugriff auf dieses Netzwerk und die darin befindlichen Systeme sollte technisch derart eingeschränkt sein, dass ausschließlich legitime Benutzer und Geräte Zugang erhalten.

Entsprechende Sicherheitsmaßnahmen sind von hoher Relevanz, da Angreifer mit logischem Zugang zum Netzwerk eine große Bedrohung darstellen:

- Daten, die im Kontext des Fachverfahrens erstellt und verarbeitet werden, können unverschlüsselt über das Netzwerk übertragen werden. Ein Angreifer mit Zugang zur Netzwerkinfrastruktur könnte diese Daten abhören oder manipulieren.
- Der Angreifer könnte Systeme im lokalen Netzwerk kompromittieren, die sonst nicht auf diese Weise aus dem Internet angreifbar wären, beispielsweise, weil der Zugriff durch eine Firewall verhindert wäre. Die Kompromittierung eines Systems, das selbst nicht direkt am Betrieb des Fachverfahrens beteiligt ist, kann dennoch ein großes Risiko darstellen, da das kompromittierte System für Folgeangriffe missbraucht werden kann. Denkbar wäre beispielsweise die Kompromittierung eines IP-Telefons, das in der Folge wiederrum für Angriffe auf Client-PCs verwendet wird.

Unabhängig von der Größe des Betreibers und der Anzahl der im Netzwerk befindlichen Geräte haben die folgenden Maßnahmen die höchste Priorität:

- 3.1 Client-Authentifizierung
- 3.2 VPN
- 3.3 Perimeter-Firewall
- 3.7 Verschlüsselung der Netzwerkkommunikation

Die Maßnahme „3.5 Isolation virtueller Teilnetze“ hat darüber hinaus die nächst höhere Priorität für Betreiber, die eine größere Anzahl unterschiedlicher Netzwerkteilnehmer hat oder der Schutzbedarf der zu verarbeitenden Daten besonders hoch ist.

3.1 Client-Authentifizierung

Eine Maßnahme, um zu erreichen, dass ausschließlich berechtigte Benutzer am Netzwerk teilnehmen, ist die sogenannte Client-Authentifizierung. Der Standard IEEE 802.1X ist eine gängige Möglichkeit dies umzusetzen.

Das Verfahren beruht darauf, dass jeder Netzwerkzugang, wie Switches, VPN-Gateways, oder Wifi-Access-Points eine Authentifizierung des Teilnehmers einfordern. Kann der Teilnehmer sich nicht erfolgreich als legitimer Nutzer authentifizieren, so wird der Zugriff auf das lokale Netzwerk vom Netzwerkzugangsgerät verweigert. Die Authentifizierung erfolgt in vielen Fällen zentral über einen RADIUS-Server. Switches und andere Netzwerkzugangsgeräte

übernehmen also die Zugangsprüfung nicht direkt selbst, sondern leiten diese nur an den RADIUS-Server weiter. Insbesondere im Kontext von Active Directory bietet sich für diesen Zweck der Betrieb eines Network Policy Servers (NPS) an, der die Aufgabe eines RADIUS-Servers übernehmen kann. Der NPS kann an den Domain-Controller angebunden werden und damit für die Client-Authentifizierung auf die Benutzer- und Geräteverwaltung der Windows-Domäne zurückgreifen. Dies kann den Aufwand zur Verwaltung von Benutzern und Benutzerrechten reduzieren.

Ein alternativer Ansatz zur Client-Authentifizierung im Netzwerk sind MAC-Filter, die nur Geräte mit zulässiger MAC-Adresse zum Netzwerk zulassen. Dieser Ansatz ist dem eingangs beschriebenen Ansatz auf Grundlage von IEEE 802.1X deutlich unterlegen, da MAC-Adressen beliebig veränderbar sind und in vielen Fällen ein Angreifer über Möglichkeiten verfügt, in einem Netzwerk zulässige Adressen mitzuhören und diese dann selbst anzunehmen. MAC-Filter stellen daher eine Lösung dar, die besser ist als gar keine Client-Authentifizierung, die klare Empfehlung ist jedoch dort wo es technisch möglich ist einen stärkeren Ansatz zu wählen, wie den eingangs beschriebenen Ansatz auf Grundlage von IEEE 802.1X.

Grundsätzlich sind andere technische Umsetzungen als IEEE 802.1X für die Client-Authentifizierung am Netzzugang auch möglich, jedoch sollten sie den gleichen Sicherheitsanforderungen wie der eingangs skizzierten Lösung genügen.

Weitere Informationen zum Network Policy Server:

- https://docs.microsoft.com/de-de/windows-server/networking/technologies/nps/nps-top

Relevante Angriffe:
A1.5: Ausnutzen einer Schwachstelle im Betriebssystem oder Anwendungssoftware
A2.2: Ausnutzen einer Schwachstelle im Betriebssystem oder Dienstsoftware
A3.2: Logischer Zugriff auf die Datenübertragung

3.2 VPN

Unter besonderen Umständen kann es erforderlich sein, dass Benutzer den Client-PC für die Ausführung des Fachverfahrens nicht beim Betreiber vor Ort an das lokale Netzwerk anbinden, sondern stattdessen entfernt über das Internet auf den Datenbankserver zugreifen. Möglicherweise sollen Benutzer auch aus dem Internet auf einen Terminalserver zugreifen können, der wiederum zur Ausführung des Fachverfahrens verwendet wird, siehe Abschnitt 4.9. Dies kann beispielsweise bei Reisetätigkeiten, oder bei der Arbeit von zu Hause der Fall sein.

In einer solchen Situation wird dringend empfohlen, die Verbindung zum Datenbankserver, Terminalserver oder gegebenenfalls auch anderen Systemen, wie zum Beispiel dem Mailserver, so technisch zu sichern, dass ein Angreifer die übertragenen Daten nicht im Klartext abhören kann, unbemerkt Änderungen vornehmen kann, oder sich selbst als legitime Datenquelle ausgeben kann. Es gilt hier also bei der Verbindung über die lokale Netzwerkgrenze die Vertraulichkeit, Integrität und Authentizität der Datenübertragung sicherzustellen.

Ein virtuelles privates Netzwerk (VPN) stellt eine Lösungsmöglichkeit dar, dies für die oben erwähnten Anwendungsfälle zu erreichen. Hierbei wird beim Betreiber im lokalen Netzwerk ein VPN-Gateway betrieben, das als Netzwerkzugang für entfernte Benutzer über das Internet verfügbar ist. Das VPN-Gateway wiederrum könnte für die Client-Authentifizierung auf einen NPS zurückgreifen, der an den

Domänen-Controller angebunden ist und damit auf die Benutzerverwaltung der Windows-Domäne zurückgreifen kann, um zu entscheiden, ob ein Teilnehmer Zugang zum lokalen Netzwerk erhalten darf.

Nach erfolgreicher Authentifizierung besteht eine kryptographisch gesicherte Verbindung und der Benutzer kann mit dem Client-PC über die VPN-Verbindung auf interne Dienste, wie Terminal-, Datenbank- und Mailserver, so zugreifen, als wäre der Client-PC lokal vor Ort an das Netzwerk angeschlossen.

Weitere Informationen zum Network Policy Server:

- https://docs.microsoft.com/de-de/windows-server/networking/technologies/nps/nps-top

Relevante Angriffe:
A3.2: Logischer Zugriff auf die Datenübertragung

3.3 Perimeter-Firewall

Der Übergang zwischen dem lokalen Netzwerk des Betreibers und dem öffentlichen Internet sollte durch eine Firewall geschützt sein. Die Firewall dient hierbei zwei Zielen.
Zum einen sollen unerwünschte Verbindungen von außen blockiert werden. Beispielsweise soll es einem Angreifer nicht möglich sein, direkt eine Verbindung aus dem Internet zum Datenbankserver des Fachverfahrens aufzubauen. Jedes aus dem Internet erreichbare System im lokalen Netzwerk stellt ein mögliches Einfallstor dar, wenn es aufgrund von Sicherheitslücken, Fehlkonfigurationen oder schwacher Zugangsdaten von einem Angreifer kompromittiert werden kann. Die Firewall kann die Angriffsfläche erheblich reduzieren, wenn der Zugriff auf alle Geräte kategorisch blockiert wird, die nicht für ihre Zweckerfüllung aus dem Internet erreichbar sein müssen.

Zum anderen dient die Firewall dem Zweck, unerwünschte Verbindungen vom lokalen Netzwerk in das öffentliche Internet zu blockieren. Unter anderem soll damit der Möglichkeitsraum eingeschränkt werden, der einem Angreifer zur Verfügung steht, wenn er bereits logischen oder physischen Zugriff auf ein lokales Gerät erlangt hat. Beispielsweise könnte die Firewall die Verbindungsmöglichkeiten des Datenbankservers derart einschränken, dass ausschließlich Verbindungen zu Domains erlaubt sind, die für Softwareupdates erforderlich sind, während alle anderen Verbindungen untersagt werden. In der Folge bedeutet dies, dass selbst dann, wenn es einem Angreifer gelingen sollte, Schadsoftware auf dem Datenbankserver zur Ausführung zu bringen, diese keine Datenbankinhalte direkt an einen unbekannten Server übertragen kann.
Für die technische Umsetzung gibt es ein breites Spektrum software- und hardwarebasierter Lösungen von einer Vielzahl unterschiedlicher Hersteller, sowie Open-Source-Lösungen. Die Auswahl einer geeigneten Lösung und die Erstellung angepasster Filterregeln muss individuell vom jeweiligen Betreiber durchgeführt werden.

Allgemein gilt die Empfehlung, Filterregeln so zu gestalten, dass sie so restriktiv wie möglich sind, und nur das explizit erlauben, was zur Zweckerfüllung der Systeme im Netzwerk erforderlich ist.

Relevante Angriffe:
A1.5: Ausnutzen einer Schwachstelle im Betriebssystem oder Anwendungssoftware

A2.2: Ausnutzen einer Schwachstelle im Betriebssystem oder Dienstsoftware
A3.2: Logischer Zugriff auf die Datenübertragung

3.4 Host-basierte Firewall

Die Perimeter-Firewall stellt eine Lösung dar, um an der Netzwerkgrenze zwischen dem lokalen Netz und dem öffentlichen Internet eingehende und ausgehende Verbindungen einzuschränken. Als weiteren Layer in einem Sicherheitskonzept bietet sich der zusätzliche Einsatz von host-basierten Firewalls an. Diese können für jeden Host individuelle Filterregeln durchsetzen und können auch dann Schutz vor Fremdzugriff bieten, wenn die Perimeter-Firewall umgangen wurde. Beispielsweise bietet es sich an, dass Client-PCs, die das Fachverfahren ausführen, ausschließlich Verbindungen akzeptieren, die sie selbst angefragt haben, beispielsweise für Softwareupdates, oder die von Systemen kommen, die sich erfolgreich an der Windows-Domäne angemeldet haben und somit als vertrauenswürdig gelten.

Eine entsprechend konfigurierte host-basierte Firewall kann daher auch die Ausnutzung von Schwachstellen im Betriebssystem und Anwendungssoftware verhindern, wenn bestimmte Verbindungsanfragen gar nicht erst zugelassen werden, und somit eine angreifbare Funktion in einer Software gar nicht zur Verarbeitung von zugesendeten Daten gelangt, was die Voraussetzung für die Ausnutzung der Sicherheitslücke wäre.

Entsprechende Hinweise für die Umsetzung mit der Windows Firewall:

- https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-firewall/restrict-access-to-only-trusted-devices

Relevante Angriffe:
A1.5: Ausnutzen einer Schwachstelle im Betriebssystem oder Anwendungssoftware
A2.2: Ausnutzen einer Schwachstelle im Betriebssystem oder Dienstsoftware

3.5 Isolation virtueller Teilnetze

Bei vielen Betreibern der Fachverfahren ist davon auszugehen, dass die lokalen Netzwerke nicht ausschließlich Geräte und Benutzer beinhalten, die zum Betrieb des Fachverfahrens gehören. Stattdessen gilt hier die Annahme, dass noch weitere Netzwerkteilnehmer vorhanden sind, beispielsweise IP-Telefone, PCs, die kein Fachverfahren ausführen, sowie gegebenenfalls noch weitere Serverdienste.

Je mehr Teilnehmer das Netzwerk umfasst, die nicht direkt mit dem Fachverfahren in Verbindung stehen, umso mehr bietet es sich an, Teilnehmergruppen in virtuelle Teilnetze (VLANs) zu unterteilen. Das Ziel, das damit erreicht werden soll, ist den Möglichkeitsraum für einen Angreifer einzuschränken, der sich illegitim Zugang zum Netzwerk verschafft hat, oder einen legitimen Netzwerkteilnehmer kompromittiert hat. Ohne eine Unterteilung in VLANs könnte ein einziger Netzwerkteilnehmer Angriffsversuche auf alle anderen Teilnehmer im Netzwerk starten. In der Folge könnte eine einzige Sicherheitslücke, beispielsweise in einem IP-Telefon, zum Einfallstor in das gesamte Netzwerk werden. Die Unterteilung in VLANs kann dies verhindern, indem ausschließlich Verbindungen zwischen Teilnehmern des gleichen VLANs zugelassen werden, und Verbindungsversuche von einem VLAN zu Teilnehmern eines anderen VLANs nicht weitergeleitet werden. Beispielsweise wäre es so möglich, alle Client-PCs und Datenbankserver, die für Fachverfahren benutzt

werden in einem VLAN unterzubringen, während IP-Telefone in einem eigenen VLAN untergebracht werden. Ein kompromittiertes IP-Telefon kann dadurch gehindert werden, Angriffe auf den Datenbankserver durchzuführen, oder den Netzwerkverkehr zu belauschen.
Die technische Umsetzung kann auf mehreren Wegen erfolgen. Eine Möglichkeit ist, die Konfiguration von VLANs direkt mit Switches umzusetzen. Diese können beispielsweise einem Netzwerkport ein bestimmtes VLAN zuweisen, oder auf Basis von IEEE 802.1Q auch mehrere VLANs pro Port unterstützen. Eine weitere Möglichkeit besteht darin, Netzwerkteilnehmer auf unterschiedliche Domänen aufzuteilen, und diese dann logisch voneinander zu isolieren.
Mehr Hinweise zur Domänen-Isolation:

- https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-firewall/domain-isolation-policy-design

Relevante Angriffe:
A1.5: Ausnutzen einer Schwachstelle im Betriebssystem oder Anwendungssoftware
A2.2: Ausnutzen einer Schwachstelle im Betriebssystem oder Dienstsoftware
A3.2: Logischer Zugriff auf die Datenübertragung

3.6 Isolation des Datenbankservers

Der Datenbankserver beinhaltet die sensitiven Daten der Fachverfahren, daher ist der Schutz des Systems von besonderer Bedeutung. Neben den anderen hier aufgeführten Maßnahmen kann ein weiterer Baustein in einem Sicherheitskonzept die Durchsetzung einer Serverisolationsrichtlinie sein. Hierbei kann per Active Directory festgelegt werden, dass der Datenbankserver ausschließlich Verbindungen annehmen darf, die von authentifizierten Teilnehmern initiiert werden, die einer bestimmten Netzwerkzugriffsgruppe zugewiesen wurden. Alle Client-PCs, die Fachverfahren ausführen, müssten entsprechend zu der legitimierten Netzwerkzugriffsgruppe hinzugefügt werden. Damit ließe sich eine Zugangsbeschränkung zwischen Netzwerkteilnehmern realisieren, die noch feingranularer ist, als die Unterteilung in VLANs.
Mehr Informationen zur Serverisolationsrichtlinie:

- https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-firewall/server-isolation-policy-design
- https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/planning-network-access-groups

Relevante Angriffe:
A2.2: Ausnutzen einer Schwachstelle im Betriebssystem oder Dienstsoftware

3.7 Verschlüsselung der Netzwerkkommunikation

Eine ungesicherte Datenverbindung zwischen Client-PC und Datenbankserver, oder gegebenenfalls auch anderen Systemen, bietet eine Angriffsfläche für ein breites Spektrum von Angriffen. So kann ein Angreifer auf dem Transportweg Daten mitlesen und manipulieren, oder sich fälschlicherweise als legitimer Kommunikationspartner ausgeben und Daten direkt vom Client-PC empfangen, oder dem Client-PC zusenden.

Zum Schutz der Vertraulichkeit, Integrität und Authentizität von Datenübertragungen im lokalen Netzwerk wird daher empfohlen, kryptographisch gesicherte Verbindungen zu verwenden.

Für den Betrieb eines Fachverfahrens ist im Besonderen die Verbindung zwischen Client-PC und Datenbankserver von Bedeutung. Eine Möglichkeit, die Nerzwerkkommunikation zwischen diesen Systemen zu schützen, ist der Einsatz von TLS. Im Kontext einer Active Directory Domäne kann ein Serversystem die Rolle einer vertrauenswürdigen Zertifizierungsstelle übernehmen, die von allen Clients der Domäne als legitimer Vertrauensanker akzeptiert wird. Der Datenbankserver kann von dieser Zertifizierungsstelle ein Zertifikat anfordern und den privaten Schlüssel lokal verwahren. Der Datenbankdienstprozess auf dem Datenbankserver muss dann so konfiguriert werden, dass er ausschließlich TLS-gesicherte Verbindungen zulässt und für den Verbindungsaufbau auf das zuvor ausgestellte Zertifikat zurückgreift. Wenn der Client-PC dann eine Verbindung zum Datenbankserver aufbaut, signalisiert dieser, dass ausschließlich TLS-Verbindungen akzeptiert werden. Sofern der Client-PC TLS-Verbindungen aufbauen kann, was in aller Regel der Fall sein sollte, wird dieser das Zertifikat des Servers erhalten, prüfen, und nach erfolgreicher Prüfung anschließend den Datenaustausch über TLS mit dem Datenbankserver fortsetzen. Hierfür sollten in der Regel keine Konfigurationsänderungen am Client-PC nötig sein.

Es wird dennoch empfohlen, sofern dies technisch umsetzbar ist, beispielsweise mit einer Host-basierten Firewall den Client-PC zusätzlich so zu konfigurieren, dass dieser ausschließlich kryptographisch gesicherte Verbindungen zur Datenbank aufbauen kann. Diese Maßnahme dient der Verhinderung von Man-in-the-Middle-Angriffen, wie beispielsweise einer Downgrade-Attack, für die ein Fachverfahren sonst möglicherweise angreifbar sein könnte.

Unabhängig von der konkreten Umsetzung ist stets darauf zu achten, dass aktuelle Kommunikationsprotokolle zum Einsatz kommen. Der TLS-Standard wird ebenso wie viele andere Sicherheitsstandards in diesem Kontext regelmäßig aktualisiert und sollte stets in der aktuellsten Version verwendet werden. Client-PC und Server können entsprechend so konfiguriert werden, dass sie ausschließlich bestimmte Versionen, zum Beispiel von TLS verwenden, um den Einsatz veralteter Protokolle zu verhindern.

Relevante Angriffe:
A3.1: Physischer Zugriff auf die Datenübertragung
A3.2: Logischer Zugriff auf die Datenübertragung

3.8 Physische Zugriffskontrolle für Netzwerk

Eine wichtige Voraussetzung für lokale Angriffe im Netzwerk ist der physische Zugang zur Netzwerkinfrastruktur. Ein Baustein eines Sicherheitskonzepts sollte daher auch die physische Zugriffskontrolle zu Netzwerkschnittstellen sein.
Ein Aspekt davon ist der physische Schutz von Übertragungswegen. Im Falle eines Drahtlosnetzwerks sollte die Sendeleistung entsprechend derart reguliert werden, dass überall dort, wo ein Netzwerkzugang zur Aufgabenerfüllung erforderlich ist eine ausreichende Empfangsqualität gewährleistet ist, jedoch möglichst nicht außerhalb des benötigten Bereichs, beispielsweise auf der gegenüberliegenden Straßenseite des Betreibers. Für kabelgebundene Netzwerke gilt es analog sicherzustellen, dass die Übertragungskabel vor Fremdzugriff geschützt sind, beispielsweise in gut gesicherten Kabelschächten, oder ausschließlich in abschließbaren Räumlichkeiten.

Neben dem Schutz der Übertragungswege kann ein weiterer Aspekt der physische Schutz von Netzwerkports sein. Es gibt dedizierte Hardwarelösungen, die physisch verhindern, dass ein Netzwerkkabel vom Endgerät getrennt wird. Im betrachteten Kontext könnte damit verhindert werden, dass der Client-PC kurzzeitig vom Netzwerk getrennt wird um Zusatzhardware zwischenzuschalten, die den Netzwerkverkehr zwischen Client-PC und anderen Systemen abhört. Ebenso wird dadurch verhindert, dass das Anschlusskabel vom Client-PC getrennt wird, um stattdessen Hardware des Angreifers für weitere Angriffe an das Netzwerk anzuschließen. Daneben gibt es weitere Hardwarelösungen, um ungenutzte Netzwerkports physisch zu blockieren. Dadurch kann verhindert werden, dass ein lokaler Angreifer eigene Netzwerkkabel an vorhandene Ports anschließt. Der hier beschriebene Schutz von Kabelanschlüssen kann in der Regel durch physische Zerstörung oder mit spezieller Hardware umgangen werden, dennoch stellen diese Maßnahmen eine Hürde dar, die den Aufwand für Angriffe erhöht.

Relevante Angriffe:
A3.1: Physischer Zugriff auf die Datenübertragung

4
Hostsicherheit

Ergänzend zu den im vorherigen Kapitel empfohlenen Maßnahmen zur Netzwerksicherheit werden in diesem Kapitel Maßnahmen zur Hostsicherheit präsentiert. Hierbei treffen wir die Annahme, dass Hostsysteme Windows 10 Professional, oder eine funktional umfangreichere Version von Windows 10 verwenden.

Insbesondere die Maßnahmen 4.1 bis 4.12 sind für alle Betreiber empfehlenswert, unabhängig von der Anzahl der im Netzwerk befindlichen Geräte. Sie entsprechen dem Stand der Technik und sollten von jedem Betreiber in Betracht gezogen werden. Die höchste Priorität haben die folgenden Maßnahmen:

- 4.1 Logische Zugriffskontrolle für PCs und Server
- 4.2 Passwortrichtlinien
- 4.3 Planmäßige Softwareupdateprozesse
- 4.10 Automatische Datensicherung
- 4.12 Physische Zugriffskontrolle für PCs und Server

4.1
Logische Zugriffskontrolle für PCs und Server

Eine fundamentale Sicherheitsmaßnahme, die in den meisten IT-Infrastrukturen Anwendung findet, ist die Zugriffsbeschränkung bei der Anmeldung an einem PC oder Server. Das Ziel hierbei ist es, unbefugten Personen den Zugang zur Software zu verwehren, wenn das jeweilige System kurzfristig unbeobachtet ist.
Weiterführend kann die Authentifizierung individueller Benutzer genutzt werden, um benutzer- oder rollenbasierte Sicherheitsrichtlinien durchzusetzen. Einer Rolle „Administrator“ können beispielsweise weitreichende Zugriffsrechte auf die IT-Infrastruktur gewährt werden, während die Rolle „Gast“ mit möglichst wenigen Rechten versehen ist.
Für die Benutzerauthentifizierung bieten sich die Möglichkeit der Ein-Faktor-Authentifizierung, sowie Lösungen für die Mehr-Faktor-Authentifizierung an:

- Option 1: Passwortschutz

  Die Benutzerauthentifizierung durch Passwort ist eine vielerorts gängige Ein-Faktor-Authentifizierung, die auf „Wissen“ beruht – jeder, der in Kenntnis des Passworts gerät, kann sich als der jeweilige Benutzer authentifizieren.

- Option 2: Zugriffstoken

  Die Authentifizierung erfolgt durch eine Kombination der beiden Faktoren „Wissen“ und „Besitz“. Eine übliche Umsetzung erfolgt mithilfe von Smartcards, deren Verwendung nur mit geheimer PIN möglich ist. Ein Angreifer muss so nicht nur in Kenntnis der PIN gelangen, sondern auch physischen Zugriff auf die Smartcard erhalten, um sich als der jeweilige Benutzer authentifizieren zu können.

Beide der oben aufgeführten Optionen sind gängige Lösungen zur logischen Zugriffskontrolle auf PCs und Server. Sofern in der praktischen Umsetzung möglich, ist jedoch die Mehr-Faktor-Authentifizierung der Ein-Faktor-Authentifizierung vorzuziehen, da diese in der Regel eine deutlich größere Hürde für Angreifer darstellt.

Mehr Informationen zum Einsatz von Smartcards im Umfeld von Windows-Netzwerkinfrastrukturen:

- https://docs.microsoft.com/de-de/windows/security/identity-protection/smart-cards/smart-card-how-smart-card-sign-in-works-in-windows
- https://support.microsoft.com/de-de/help/281245/guidelines-for-enabling-smart-card-logon-with-third-party-certificatio

Im Allgemeinen kann auch auf biometrische Verfahren zurückgegriffen werden. In diesen Fällen ist jedoch wichtig, auf eine sichere Speicherung der biometrischen Merkmale zu achten, da diese sensitiv sind und in unterschiedlichen Verfahren mit unterschiedlichem Schutzbedarf zu Anwendung kommen könnten. Ebenso von großer Bedeutung ist, dass die eingesetzte Hardware zur Erkennung biometrischer Merkmale schwer zu täuschen ist. In der Vergangenheit gab es beispielsweise Angriffe auf Smartphones, bei denen ein gefälschter Fingerabdruck zur Entsperrung des Geräts verwendet werden konnte. Biometrische Merkmale sind nicht austauschbar wie Passwörter oder Zugriffstoken, die Sicherheit beruht einzig auf der Qualität der eingesetzten Hardware.

Relevante Angriffe:
A1.1: Social Engineering
A1.7: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A2.1: Social Engineering
A2.3: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren
A5: Manipulation des Fachverfahrens auf dem Client-PC

4.2 Passwortrichtlinien

Wie oben bereits erläutert dient die Benutzerauthentifizierung auch zur Durchsetzung eines Rechtesystems, das Benutzer und ihre jeweiligen Rollen unterscheidet. Für einen Angreifer kann es daher lohnenswert sein, sich illegitim als ein Benutzer mit weitreichenden Rechten zu authentifizieren. Um insbesondere auch beim Einsatz einer Ein-Faktor-Authentifizierung durch Passwort derartige Angriffe zu erschweren, empfiehlt sich die Durchsetzung einer Passwortrichtlinie, die unter anderem verhindert, dass Benutzer leicht zu erratende Passwörter wählen.

Hinweise zur Gestaltung einer Passwortrichtlinie stellt unter anderem das BSI bereit. Informationen hierzu finden sich zum Beispiel in den Umsetzungshinweisen des BSI zum IT-Grundschutz-Kompendium, die regelmäßig aktualisiert werden:

- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html

Umsetzungshinweise des BSI zur Passwortrichtlinie in Active Directory für Edition 2019 des IT-Grundschutz-Kompendiums:

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.pdf?__blob=publicationFile&v=10 (Seite 420)

Allgemeine Informationen zur Durchsetzung einer Passwortrichtlinie in Windows-Domänen:

- https://docs.microsoft.com/de-de/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

Relevante Angriffe:
A1.7: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A2.3: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren
A5: Manipulation des Fachverfahrens auf dem Client-PC

4.3 Planmäßige Softwareupdateprozesse

Jede Software, die auf dem Client-PC, oder einer Serverinstallation zum Einsatz kommt, sollte regelmäßig aktualisiert werden, um die neuesten Fehlerbehebungen zu erhalten. Dies umfasst explizit nicht nur das Betriebssystem selbst, sondern auch Anwendungssoftware, wie PDF-Reader, Mailclient, usw. Jede Software, die über eine bekannte Sicherheitslücke verfügt, kann potenziell von einem Angreifer ausgenutzt werden. Je nach Software und Hersteller können sich die Updateprozesse unterscheiden, daher sollte individuell für jede Softwareinstallation eine geeignete Vorgehensweise ausgearbeitet werden.

Für die administrativ organisierte Verteilung von Betriebssystemupdates für Windows-Systeme gibt es die sogenannten Windows Server Update Services (WSUS). Mithilfe von WSUS können Deploymentstrategien umgesetzt werden, die auf die Anforderungen des jeweiligen Betreibers angepasst sind. Beispielsweise kann in einer größeren Netzwerkinfrastruktur ein sogenanntes Ring-Deployment zum Einsatz kommen. Hierbei werden alle Systeme, die es mit Updates zu versorgen gilt, in unterschiedliche Ringe eingeteilt. Die Systeme in den einzelnen Ringen werden dann entsprechend zeitlich versetzt mit Betriebssystemupdates versorgt, um eventuellen Schaden und Zusatzaufwand zu begrenzen, der in Fällen entstehen kann, in denen durch Betriebssystemupdates einzelne Softwareinstallationen oder gesamte Systeme funktional eingeschränkt werden.

Eine typische Aufteilung erfolgt in drei unterschiedliche Ringe. Der erste Ring umfasst eine geringe Menge an Systemen, z.B. 10%, und erhält als erstes neue Betriebssystemupdates. Wenn nach dem Verteilen neuer Updates in dem Ring kein systematisches Problem entstanden ist, kann der nächste Ring mit Updates versorgt werden, der beispielsweise 80% der Systeme umfasst. Die verbliebenen 10% der Systeme könnten dann in einem dritten Ring sein, der als letztes mit Updates versorgt wird. Hier könnten beispielsweise Systeme zusammengefasst sein, die wenig exponiert sind, aber deren Funktion im internen Netzwerk von großer Bedeutung ist. Die hier dargestellte Aufteilung in Ringe ist ausschließlich als Beispiel zur Veranschaulichung gedacht. Jeder Betreiber muss ein entsprechendes Konzept ausarbeiten, das die individuellen Anforderungen berücksichtigt.

Insbesondere in Netzwerken, die eine geringe Anzahl von Systemen umfassen, können deutlich simplere Deploymentstrategien angemessen sein. Hier könnte es beispielsweise genügen, in einer ersten Updatephase einzelne besonders kritische

Systeme auszuschließen, und diese erst dann zu aktualisieren, wenn alle anderen Systeme ohne Probleme aktualisiert und betrieben werden konnten.

Weitere Informationen zu WSUS im Allgemeinen:

- https://docs.microsoft.com/de-de/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

Hinweise zum Optimieren des Deployments von Betriebssystemudpates für Windows:

- https://www.microsoft.com/en-us/download/details.aspx?id=101056

Relevante Angriffe:
A1.4: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber
A1.5: Ausnutzen einer Schwachstelle im Betriebssystem oder Anwendungssoftware
A2.2: Ausnutzen einer Schwachstelle im Betriebssystem oder Dienstsoftware
A2.5: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber

4.4 Einschränkung der Benutzerrechte am Client-PC

Im Allgemeinen ist es empfehlenswert, Benutzerkonten nur mit den Rechten zu versehen, die der Benutzer für seine Tätigkeit benötigt, und alle weiteren Rechte zu verweigern. Im Kontext von Active Directory ist es möglich, die Verwaltung von Benutzerrechten zentral per Gruppenrichtlinie durchzuführen. In vielen Fällen kann es beispielsweise empfehlenswert sein, dem Benutzer die Möglichkeit zu entziehen, neue Software zu installieren, Firewall-Regeln zu ändern, oder auf die Systemsteuerung zuzugreifen. Welche Rechte der jeweilige Anwender jedoch im Detail benötigt hängt von der Tätigkeit ab und muss vom jeweiligen Betreiber festgelegt werden.

Neben dieser allgemeinen Empfehlung zur Beschränkung von Benutzerrechten gibt es eine darüberhinausgehende Lösung, die insbesondere erschweren soll, dass Angreifer auf den Programmordner des Fachverfahrens, oder den entsprechenden Prozess zur Laufzeit zugreifen können. Hierbei werden jedem Benutzer des Fachverfahrens zwei unterschiedliche Benutzerkonten zugewiesen, im Folgenden „<Benutzer>“ und „<Benutzer>-Technisch“ genannt. Das Konto „<Benutzer>“ wird vom Sachbearbeiter verwendet, um sich am Client-PC anzumelden und regulären Tätigkeiten nachzugehen, die nicht die Verwendung des Fachverfahrens betreffen. Dieses Konto verfügt entsprechend der allgemeinen Empfehlung nur über eingeschränkte Rechte. Darüber hinaus wurde diesem Konto jedoch auch explizit der Zugriff auf den Programmordner des Fachverfahrens verweigert. In der Folge kann der Sachbearbeiter, der sich als „<Benutzer>“ angemeldet hat, nicht mehr direkt auf die darin befindlichen Dateien zugreifen, oder das Fachverfahren starten. Sollte dieser Benutzer also unbeabsichtigt oder unwissentlich Schadsoftware ausführen, so kann diese weder lesend noch schreibend auf die Programmdateien zugreifen, da diese mit den gleichen Rechteeinschränkungen ausgeführt würde.

Damit der Sachbearbeiter dennoch das Fachverfahren ausführen und verwenden kann, wurde das Konto „<Benutzer>-Technisch“ erstellt. Dieses Konto verfügt ebenfalls nur über eingeschränkte Rechte, jedoch wird diesem Konto explizit das Recht gestattet, auf den Programmordner des Fachverfahrens zuzugreifen. Per Whitelist kann diesem Konto die Möglichkeit genommen werden, andere Programme als das Fachverfahren zu starten. Der Sachbearbeiter, der als „<Benutzer>“ am Client-PC angemeldet ist, kann zum Start des Fachverfahrens nun

im Kontextmenü der Datei, die das Fachverfahren startet, den Eintrag „Als anderer Benutzer ausführen“ wählen, und nach erfolgreicher Authentifizierung als „<Benutzer>-Technisch“ den Prozess starten. Ebenfalls möglich ist es, eine Batch-Datei oder ein PowerShell-Skript bereitzustellen, das bereits automatisch das Fachverfahren mit dem Konto „<Benutzer>-Technisch“ startet, womit dem Benutzer der Umweg über das Kontextmenü erspart wird. Hierbei ist jedoch wichtig, keine Passwörter in diesen Dateien zu hinterlegen – der Benutzer soll auch in diesem Fall manuell die Authentifizierung als „<Benutzer>-Technisch“ durchführen müssen.

Die hier dargestellte Lösung mit zwei unterschiedlichen Benutzerkonten ist immer dann vorzuziehen, wenn die technischen und organisatorischen Gegebenheiten dies erlauben. In allen anderen Fällen, beispielsweise wenn die spezifische Implementierung des jeweiligen Fachverfahrens keine unterschiedlichen Konten zulässt, sollte zumindest der allgemeinen Empfehlung gefolgt werden und das Konto des Sachbearbeiters auf die Rechte beschränkt werden, die für die jeweilige Tätigkeit unabdingbar sind.

Relevante Angriffe:
A1.1: Social Engineering
A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren
A5: Manipulation des Fachverfahrens auf dem Client-PC

4.5 Automatisches Sperren

Die logische Zugriffskontrolle zu PCs und Serverinstallationen ist ein fundamentaler Baustein in einem Sicherheitskonzept. Das automatische Sperren eines Systems, wenn es nicht vom berechtigten Benutzer in Verwendung ist, stellt daher eine empfehlenswerte Maßnahme dar. Hierfür gibt es unterschiedliche Lösungen, die zusammen, oder auch einzeln umsetzbar sind.

Eine gängige Möglichkeit ist das automatische Sperren des Systems nach einer festgelegten Zeitspanne, in der der angemeldete Benutzer nicht aktiv mit dem System interagiert hat. Diese Maßnahme lässt sich per Gruppenrichtlinie zentral konfigurieren. Eine weitere Möglichkeit ist das automatische Sperren des Systems, wenn ein Token entfernt wird. Falls die Anmeldung am System ohnehin per Token erfolgt, siehe Sektion 4.1, so kann per Sicherheitsrichtlinie festgelegt werden, dass das Entfernen des Tokens zur Sperrung führt. Es ist auch möglich Token für die automatische Sperrung einzusetzen, die nicht zur Anmeldung verwendet werden. Mit Windows 10 sind hierfür beispielsweise Bluetooth-Geräte geeignet, die mit dem jeweiligen System gekoppelt werden, und bei der Entkoppelung beim Entfernen vom System zur Sperrung führen.
Weitere Informationen zur Sperrung per Bluetooth-Token:

- https://support.microsoft.com/de-de/help/4028111/windows-lock-your-windows-10-pc-automatically-when-you-step-away-from

Relevante Angriffe:
A1.6: Abfotografieren des Bildschirminhalts
A1.7: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A2.3: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren
A5: Manipulation des Fachverfahrens auf dem Client-PC

4.6 Malware-Erkennung auf Hostsystem

Es gibt eine Vielzahl von Möglichkeiten, wie Schadsoftware auf ein Hostsystem gelangen kann. Das Fehlverhalten des jeweiligen Benutzers ist eine dieser Möglichkeiten, beispielsweise, wenn Schadsoftware unbedacht aus dem Internet heruntergeladen und ausgeführt wird. Jedoch auch ohne Zutun des Benutzers kann Schadsoftware auf das System gelangen, etwa wenn der Angreifer eine Sicherheitslücke im Betriebssystem oder einer Anwendungssoftware ausnutzt, um Schadcode zur Ausführung zu bringen und Malware nachzuladen. Beispielsweise könnte ein Angreifer eine speziell präparierte E-Mail versenden, die beim Empfang ohne Benutzerinteraktion eine Sicherheitslücke im Mailclient ausnutzt, die die Ausführung von Code ermöglicht, und zur Installation von Schadsoftware missbraucht wird.

Um dieses Problem zu adressieren, bietet sich der Einsatz einer automatischen Malware-Erkennung an. Diese prüft fortlaufend potentiell gefährliche Dateien auf dem Client-PC, um Schadsoftware zu erkennen, bevor sie Schaden verursacht. Aktuelle Windowsversionen bieten mit Microsoft Defender Antivirus eine umfangreiche Lösung zur Erkennung von Malware auf Client-PCs und Servern. Darüber hinaus gibt es eine Vielzahl weiterer Lösungen unterschiedlicher Hersteller.

Wichtig ist, dass die jeweilige Lösung stets aktuell gehalten wird, sodass auch neue Varianten bekannter Schadsoftware erkannt werden können.

Relevante Angriffe:
A1.1: Social Engineering
A1.7: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A2.1: Social Engineering
A2.3: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A3.2: Logischer Zugriff auf die Datenübertragung
A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren
A5: Manipulation des Fachverfahrens auf dem Client-PC

4.7 Datenträgerverschlüsselung

Sowohl auf Client-PCs, wie auch auf Servern der Domäne befinden sich sensitive Daten, die vor Manipulation und unerlaubtem Fremdzugriff geschützt werden müssen. Das schließt mit ein, dass Angreifer nicht ohne Weiteres Schadsoftware auf Festplatten installieren können sollten, während diese unbeobachtet Zugriff auf die Hardware haben.

Die Festplattenverschlüsselung stellt eine gängige Maßnahme gegen lokale Angreifer dar, die vor Ort Hardware manipulieren oder entwenden können. Das System erfragt beim Start des Systems vom Anwender die Eingabe eines Kennworts, das zur Ent- und Verschlüsselung von Daten auf dem Datenträger erforderlich ist. Ohne das Kennwort können Daten nicht im Klartext gelesen, oder geschrieben werden.
Eine auf Windowssystemen gängige Lösung stellt BitLocker dar. Eine häufig verwendete Open-Source-Alternative ist VeraCrypt.

Mit Hilfe einer entsprechenden Gruppenrichtlinie kann festgelegt werden, dass auch USB-Sticks zwingend mit BitLocker verschlüsselt werden müssen. Hierdurch kann

verhindert werden, dass ein verlorener oder entwendeter USB-Stock zur Preisgabe sensitiver Daten führt.

Informationen zur Aktivierung von BitLocker:

- https://support.microsoft.com/de-de/help/4028713/windows-10-turn-on-device-encryption

Relevante Angriffe:
A1.2: Physischer Zugriff auf die Festplatte
A2.4: Physischer Zugriff auf die Festplatte
A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren
A5: Manipulation des Fachverfahrens auf dem Client-PC

4.8 Schutz von Browser und Mailclient

Es gilt die Annahme, dass der Client-PC nicht ausschließlich dem Betrieb des Fachverfahrens dient, sondern darüber hinaus auch zum Webbrowsen und E-Mail-Empfang. Sowohl der Browser, als auch der Mailclient stellen jedoch Möglichkeiten dar, wie Schadsoftware auf den Client-PC gelangen kann. Dies kann einerseits durch Zutun des jeweiligen Benutzers erfolgen, der beispielsweise unwissentlich Schadsoftware aus dem Internet herunterlädt und zur Ausführung bringt. Andererseits kann auch ohne Nachlässigkeit oder Zutun des Anwenders Schadsoftware auf den Client-PC gelangen, beispielsweise, wenn eine vom Angreifer konstruierte E-Mail oder Webseiteninhalte Sicherheitslücken in Browser oder Mailclient ausnutzen. Daher sind Maßnahmen empfehlenswert, die diesem Risiko entgegentreten.

Zum Schutz des Browsers gibt es unter anderem folgende Möglichkeiten:

- Microsoft Defender Application Guard

  Diese Funktionalität in Windowssystemen verwendet eine hardware-unterstützte Isolation zwischen dem Edge-Browser und allen anderen Teilen des Systems, um Browser-basierten Angriffen und Schadsoftware entgegenzustehen. Per Gruppenrichtlinie kann festgelegt werden, dass nicht-vertrauenswürde Webseiten von Edge ausschließlich mit Application Guard besucht werden können. Unerwünschte Änderungen am Dateisystem, wie die Installation von Schadsoftware, können dadurch verhindert werden.

  Bei Microsoft Defender Application Guard handelt es sich um ein optionales Feature, das erst mit neueren Versionen von Windows 10 Einzug gefunden hat. Daher sollte nicht ausgeschlossen werden, dass mit neuen Betriebssystemupdates Änderungen an der Funktionsweise einhergehen könnten, die sich auf die Anwendbarkeit dieser Funktionalität im hier betrachteten Kontext auswirken.

- Dedizierte VM zum Webbrowsen

  Bei dieser Lösung wird dem Anwender eine dedizierte virtuelle Maschine bereitgestellt, die zum Browsen und bei Bedarf auch zu anderen Zwecken, wie der E-Mail-Kommunikation, dient. Durch die Virtualisierung wird eine Isolation zwischen dem eigentlichen Hostsystem und der Anwendung, wie dem Webbrowser, geschaffen. Kommt es in diesem Kontext zur Ausführung

von Schadcode, so ist davon zunächst nur die virtuelle Maschine betroffen und nicht das Hostsystem mit dem Fachverfahren.

Zum Schutz des Mailclients wird empfohlen, HTML-Inhalte, ebenso wie das automatische Nachladen von Bildern und anderen Inhalten zu deaktivieren. Ebenso sollte der Mailclient die vollständige E-Mail-Adresse des Senders anzeigen, sowie die vollständigen Dateinamen der Dateianhänge (z.B. „Rechnung.pdf.exe“).

Darüber hinaus wird empfohlen, auf dem Mailserver eine Filterung durchzuführen, die einerseits auf Schadsoftware prüft, und andererseits auf unerwünschte Dateianhänge reagiert. Eine Möglichkeit ist hier, E-Mails mit unerwünschten Dateianhängen zu blockieren und so gar nicht erst zum Anwender weiterzuleiten. Eine weitere Möglichkeit kann sein, unerwünschte Dateiformate automatisch in andere Dateiformate zu konvertieren, beispielsweise Word-Dateien in PDF-Dateien, und nur diese konvertierten Dateien an Anwender weiterzuleiten. Für die technische Umsetzung dieser Maßnahmen gibt es ein sehr breites Spektrum unterschiedlicher Softwarelösungen. Die Auswahl und Konfiguration muss vom jeweiligen Betreiber vorgenommen werden.

Für alle hier dargestellten Lösungen gilt, dass diese nicht überall umsetzbar sind. Ein Grund hierfür kann schlicht sein, dass die technischen Gegebenheiten nicht vorhanden sind. Es gilt insbesondere deswegen, aber auch allgemein die dringende Empfehlung, Browser und Mailclient stets aktuell zu halten, um so stets die aktuellsten Fehlerbehebungen der Hersteller zu erhalten, siehe Sektion 4.3.

Relevante Angriffe:
A1.1: Social Engineering
A1.5: Ausnutzen einer Schwachstelle im Betriebssystem oder Anwendungssoftware
A2.1: Social Engineering
A2.2: Ausnutzen einer Schwachstelle im Betriebssystem oder Dienstsoftware

4.9 Einsatz eines Terminalservers

Eine technische Möglichkeit, um sensitive Daten und Anwendungen zu isolieren und vor unerwünschtem Zugriff zu schützen, ist der Einsatz eines Terminalservers. Hierbei steht für den Benutzer neben dem Client-PC zusätzlich ein Terminalserver bereit, der über das Netzwerk erreicht werden kann. Zum Beispiel über RDP kann der Benutzer eine Remote-Session vom Client-PC zum Terminalserver aufbauen und dort Anwendungen ausführen und Daten verarbeiten, die nicht lokal auf dem Client-PC vorliegen, sondern ausschließlich auf dem Terminalserver. Per Gruppenrichtlinie kann eingeschränkt werden, welche Anwendungen und Daten dem Benutzer auf dem Terminalserver zur Verfügung stehen. Eine Whitelist kann beispielsweise die Menge der Programme beschränken, die der Benutzer dort starten darf.

Eine Möglichkeit zum Einsatz des Terminalservers ist für die Ausführung des Fachverfahrens. Der Client-PC kann weiterhin für andere Arbeitstätigkeiten, zum Browsen und zum E-Mail-Empfang verwendet werden, während das Fachverfahren davon isoliert auf dem Terminalserver ausgeführt wird. Eine weitere Einsatzmöglichkeit ist der umgekehrte Fall, bei dem das Fachverfahren weiter auf dem Client-PC ausgeführt wird, aber alle davon trennbaren Aktivitäten auf dem Terminalserver ausgeführt werden. In beiden Fällen gibt es eine Trennung zwischen dem Fachverfahren und weiterer Anwendungssoftware, was als Maßnahme einer Reihe von Angriffen entgegensteht.

Relevante Angriffe:
A1.1: Social Engineering
A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren
A5: Manipulation des Fachverfahrens auf dem Client-PC

4.10 Automatische Datensicherung

Insbesondere für den Datenbankserver, aber auch für andere Server der Domäne und gegebenenfalls Client-PCs ist die regelmäßige Datensicherung empfehlenswert, um unbefugten Datenmanipulationen oder unerwünschtem Datenverlust entgegenzustehen. Im Falle eines Angriffs, beispielsweise mit einer sogenannten Ransomware, die aus erpresserischen Gründen Daten verschlüsselt, aber auch im Fall des Eintretens anderer unerwarteter Vorkommnisse, die zum Datenverlust führen, kann die Datensicherung dazu genutzt werden, einen Datenbestand wiederherzustellen, der zum Zeitpunkt der letzten Datensicherung aktuell war. Eine tägliche Datensicherung stellt daher in vielen Fällen eine Lösung dar, um möglicherweise entstehende Schäden zu minimieren.

Zur technischen Umsetzung besteht die Möglichkeit, auf Funktionalitäten zurückzugreifen, die Windows-Server-Installationen bereits ohne Zusatzsoftware bereitstellen. Für einen umfangreicheren Funktionsumfang steht eine Vielzahl kostenloser und kommerzieller Lösungen bereit.

Wichtig bei der Planung und Umsetzung eines Konzepts zur Datensicherung ist, die konkreten Ziele zu formulieren und technisch zu adressieren. Der Schutz vor Ransomware ist beispielsweise in vielen Fällen ein relevantes Ziel, das jedoch nur dann erreicht werden kann, wenn der Datensicherungsbestand vor dem unerlaubten Fremdzugriff durch die Schadsoftware geschützt ist. Eine Lösungsmöglichkeit neben vielen weiteren ist die Verwendung eines Speichermediums, das nur einmalig beschreibbar ist und nach erfolgter Datensicherung keine Datenmanipulation mehr zulässt.

Informationen zur Windows Server-Funktionalität für Backups:

- https://docs.microsoft.com/de-de/windows-server-essentials/manage/set-up-or-customize-server-backup

Relevante Angriffe: Alle Angriffe oder Ereignisse, die die Integrität von Daten gefährden, oder zu Datenverlust führen

4.11 Secure Boot

In der Vergangenheit gab es Schadsoftware und gezielte Angriffe auf Hostsysteme, die Software manipuliert haben, die bereits früh beim Start des Systems zur Ausführung gelangt, wie etwa Bootloader, oder Firmwaretreiber. Das Ziel des Angreifers hierbei war, möglichst früh die Kontrolle über das System zu erlangen, bevor Betriebssystem oder Anwendungssoftware dem entgegenstehen konnten.

Secure Boot ist eine mit UEFI 2.3.1 erschienene Funktionalität, die sicherstellen soll, dass ausschließlich Software am Start des Hostsystems beteiligt ist, die unverändert vom jeweiligen Hersteller stammt. Die Überprüfung beim Startvorgang erfolgt mithilfe kryptographischer Signaturen, die von den jeweiligen Herstellern für ihre

Softwarekomponenten erstellt wurden, und zum Erkennen unerwünschter Manipulationen verwendet werden können.

Die Konfiguration des BIOS / UEFI sollte durch ein Passwort geschützt sein, um beispielsweise die unerwünschte Deaktivierung von Secure Boot zu verhindern.

Der Einsatz von Secure Boot steht einem Angriff entgegen, bei dem ein Angreifer über physischen Zugriff auf die Festplatte Schadsoftware installiert, die während des Systemstarts bereits die Kontrolle über das System übernimmt, bevor das Betriebssystem und gegebenenfalls Antivirensysteme zur Ausführung gelangen.

Mehr Informationen zu Secure Boot auf Windowssystemen:

- https://docs.microsoft.com/de-de/windows-hardware/design/device-experiences/oem-secure-boot

Relevante Angriffe:
A1.2: Physischer Zugriff auf die Festplatte
A2.4: Physischer Zugriff auf die Festplatte

4.12 Physische Zugriffskontrolle für PCs und Server

Der unerlaubte Fremdzugriff auf Hard- und Software stellt aus einer Vielzahl verschiedener Gründe ein relevantes Angriffsszenario dar, wie beispielsweise:

- Installation eines Hardware-Keyloggers könnte genutzt werden und Tastatureingaben abzufangen.
- Zugriff auf die Festplatte könnte genutzt werden, um Schadsoftware zu installieren.
- Die Hardware, und somit auch die darauf hinterlegten Daten, könnte entwendet werden.

Es wird daher dringend empfohlen, Server und Client-PCs in abschließbaren Räumlichkeiten aufzubewahren und zu betreiben. Dies gilt auch für aus dem Betrieb genommene Hardware, die, sofern sie nicht ordnungsgemäß entsorgt wurde, sensitive Informationen preisgeben könnte. Der Zugriff zu den Räumlichkeiten sollte nur legitimiertem Personal gestattet sein.

Relevante Angriffe:
A1.2: Physischer Zugriff auf die Festplatte
A1.3: Physischer Zugriff auf Eingabegeräte
A1.4: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber
A1.6: Abfotografieren des Bildschirminhalts
A1.7: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A2.3: Manipulation der Gruppenrichtlinie auf dem Domaincontroller
A2.4: Physischer Zugriff auf die Festplatte
A2.5: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber
A3.1: Physischer Zugriff auf die Datenübertragung

4.13 Bildschirmschutz

Der Client-PC wird zur Erfassung, Darstellung und Bearbeitung sensitiver Daten verwendet. Ein umfassendes Sicherheitskonzept zum Schutz der Daten sollte

Maßnahmen beinhalten, die einen lokalen Angreifer daran hindern, optisch ein Bild der Daten zu erhalten, während diese auf dem Bildschirm dargestellt werden. Hierfür ist es empfehlenswert, den Bildschirm derart auszurichten, dass er vom Sachbearbeiter eingesehen werden kann, jedoch nicht durch unbefugte Personen innerhalb der Räumlichkeit, oder durch Fenster von außerhalb. Zusätzlich kann durch geeignete Blenden und Schutzfolien der Blickwinkel eingeschränkt werden, der zum Betrachten des Bildschirminhalts erforderlich ist.

Relevante Angriffe:
A1.6: Abfotografieren des Bildschirminhalts

4.14 Physischer Schutz von Hardwareschnittstellen

Client-PCs und Server verfügen in vielen Fällen über Hardwareschnittstellen, die zur jeweiligen Zweckerfüllung des Geräts im Einsatzkontext nicht erforderlich sind. Dazu zählen USB-Ports und Netzwerkports, aber gegebenenfalls auch weitere Schnittstellen. Potenziell wird mit jeder Schnittstelle, auf die ein Angreifer zugreifen könnte, die Angriffsfläche des jeweiligen Systems erhöht. Beispielsweise könnte ein lokaler Angreifer manipulierte Hardware in USB-Ports stecken, die Sicherheitslücken in Betriebssystemkomponenten oder Treibern ausnutzt.

Zum Zweck der Risikominimierung empfiehlt es sich, alle ungenutzten Hardwareschnittstellen physisch zu blockieren. Dies kann durch Abdeckungen erfolgen, die vor die jeweiligen Schnittstellen angebracht werden, oder mithilfe dedizierter Hardware, die für das physische Blockieren der Schnittstelle entwickelt wurde. Entsprechende Lösungen gibt es zum Beispiel für USB-Ports, wobei ein Stecker zur Blockierung verwendet wird, der ausschließlich mit Hilfe der dazugehörigen Spezialhardware wieder entfernt werden kann.

Die Blockierung von Schnittstellen verhindert nicht nur unmittelbare Angriffe durch lokale Angreifer, sondern unterbindet auch, dass Mitarbeiter unerwünscht ungeprüfte Zusatzhardware an Schnittstellen anschließen.

Relevante Angriffe:
A1.1: Social Engineering
A1.4: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber
A2.1: Social Engineering
A2.5: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber

5
Organisatorische Maßnahmen

Ergänzend zu den in den vorherigen Kapiteln bereits vorgestellten technischen Maßnahmen werden in diesem Kapitel weitere organisatorische Sicherheitsmaßnahmen empfohlen. Diese gelten für alle Betreiber unabhängig von ihrer Größe.

5.1
Eingeschränkte Softwareauswahl für PCs und Server

Jede Software, die auf einem System installiert ist, hat das Potenzial, die Angriffsfläche zu erhöhen. Es empfiehlt sich daher, die Anzahl der Softwareinstallationen auf PCs und Servern so gering wie möglich zu halten und ausschließlich Software zu installieren, die zur Zweckerfüllung notwendig ist. Das Installieren von Software sollte ausschließlich administrativen Benutzern vorbehalten sein, die vor der Installation eine Einzelfallprüfung durchführen, um sicherzustellen, dass die zu installierende Software dem Einsatzweck des jeweiligen Systems entspricht, die Software qualitativen Mindestanforderungen entspricht, und schließlich eine möglichst sichere Konfiguration vorgenommen wird.

Hinweise zur Einschränkung von Nutzerrechten, um die Installation von Software einzuschränken:

- https://social.technet.microsoft.com/wiki/contents/articles/53218.windows-10-version-1903-prevent-software-installation-by-users.aspx

Relevante Angriffe:
A1.5: Ausnutzen einer Schwachstelle im Betriebssystem oder Anwendungssoftware
A2.2: Ausnutzen einer Schwachstelle im Betriebssystem oder Dienstsoftware

5.2
Security-Awareness-Training für Mitarbeiter

Angreifer versuchen durch Social Engineering Mitarbeiter dazu zu bewegen, Tätigkeiten durchzuführen und Informationen preiszugeben, die dem Angriffsziel dienlich sind. Ein häufig vorkommendes Beispiel stellen Phishing-E-Mails dar, die auf die Preisgabe von Zugangsdaten abzielen. Ein weiteres Beispiel ist das Hinterlegen manipulierter USB-Sticks, die von Mitarbeitern gefunden werden sollen, um möglicherweise aus Neugier in Hostsysteme des Betreibers eingesteckt zu werden. Neben Social Engineering können auch Nachlässigkeiten eines Benutzers ein Sicherheitsrisiko darstellen, etwa, wenn unbedacht nicht vertrauenswürdige Software aus dem Internet heruntergeladen und auf dem Client-PC ausgeführt wird. Das umsichtige und sicherheitsbewusste Verhalten von Mitarbeitern in allen Rollen trägt daher maßgeblich zum erfolgreichen Umsetzen eines Sicherheitskonzepts bei. Ein Weg, dieses Ziel zu unterstützen, stellen regelmäßige Sicherheitsschulungen für Mitarbeiter dar. Diese müssen nicht in erster Linie das Ziel verfolgen, technisches Hintergrundwissen zu vermitteln, sondern sollen die Achtsamkeit erhöhen und den Blick für mögliche IT-Sicherheitsrisiken schärfen.

Entsprechende Schulungen können von sachkundigem Personal des Betreibers durchgeführt werden, oder alternativ durch einen externen Dienstleister erbracht werden.

Relevante Angriffe:
A1.1: Social Engineering
A2.1: Social Engineering

5.3
Externe Dritte nicht unbeobachtet mit Hardware lassen

Eine Vielzahl technischer Maßnahmen soll Angriffe unterschiedlicher Art verhindern oder zumindest erschweren. In einem mehrstufigen Sicherheitskonzept ist es trotz aller technischer Maßnahmen dennoch empfehlenswert, potenziell nicht vertrauenswürdige Personen nie unbeaufsichtigt mit Hardware zu lassen. Dies betrifft alle Client-PCs, Server, Netzwerkinfrastruktur und weitere Geräte, die vom Betreiber zur Zweckerfüllung betrieben werden. Um dieses Ziel zu erreichen, sollten alle Arbeitsabläufe geprüft und daraufhin ausgerichtet sein, dass alle nicht abgeschlossenen Räumlichkeiten, die entsprechende Hardware beinhalten, zu jedem Zeitpunkt durch Mitarbeiter des Betreibers oder vertrauenswürdige Dienstleister beaufsichtigt sind.

Relevante Angriffe:
A1.2: Physischer Zugriff auf die Festplatte
A1.3: Physischer Zugriff auf Eingabegeräte
A1.4: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber
A1.6: Abfotografieren des Bildschirminhalts
A2.4: Physischer Zugriff auf die Festplatte
A2.5: Ausnutzen einer Schwachstelle in einem Schnittstellentreiber
A3.1: Physischer Zugriff auf die Datenübertragung
A4: Herleitung von Zugangsdaten zur Datenbank aus dem Fachverfahren
A5: Manipulation des Fachverfahrens auf dem Client-PC

6 Abschluss

In diesem Dokument wurden IT-Sicherheitsrisiken beim Betrieb eines Fachverfahrens erläutert und Maßnahmen empfohlen, die entsprechend geeignet sind diese Risiken zu adressieren. Die vorgestellten Maßnahmen entsprechen dem Stand der Technik und sollten bei der Entwicklung eines Sicherheitskonzepts in Betracht gezogen werden.

Die Auswahl und Priorisierung der in diesem Dokument dargestellten Maßnahmen basiert auf der Sicherheitsexpertise der Autoren und dem besonderen Fokus auf Fachverfahren, deren Architektur der Beschreibung in Abschnitt 1.3 gleicht.

Hierbei ist wichtig zu beachten, dass weder die dargestellten Angriffswege noch die vorgestellten Sicherheitsmaßnahmen erschöpfend betrachtet wurden. Ein Restrisiko wird auch dann immer vorhanden sein, wenn weitreichende Sicherheitsmaßnahmen umgesetzt wurden. Zudem gilt es bei der Planung und Umsetzung der Maßnahmen stets die individuellen Gegebenheiten des jeweiligen Betreibers zu beachten. Dies umfasst zum Beispiel die Anzahl der Anwender, die technischen Eigenheiten der eingesetzten Fachverfahren, sowie die technischen Eigenschaften der eingesetzten Hardware. Zudem ist festzustellen, dass es eine sehr große Anzahl von Möglichkeiten gibt, die hier präsentierten Sicherheitsmaßnahmen umzusetzen. Dies ergibt sich nicht zuletzt aufgrund der Vielzahl von Herstellern, Softwarelösungen, und Konfigurationsmöglichkeiten, die für die Umsetzung in Frage kommen.

Zuletzt muss auch kontextabhängig bewertet werden, welche Sicherheitsziele für den jeweiligen Betreiber relevant sind, und welche Maßnahmen geeignet sind, die Sicherheitsziele zu adressieren. Neben der Umsetzbarkeit gilt es hierbei auch die Wirtschaftlichkeit einzelner Sicherheitsmaßnahmen zu bewerten, da in unterschiedlichen Kontexten das Verhältnis von Kosten und Nutzen unterschiedlich sein kann. In jedem Fall sollte eine derartige Bewertung jedoch systematisch erfolgen und relevante Sicherheitsziele sollten in der Betrachtung stets das Gewicht erhalten, das eine systematische Risikobewertung ergeben hat.

Aus all diesen und weiteren Gründen ist es daher erforderlich, dass jeder Betreiber ein individuelles Sicherheitskonzept gestaltet, das relevante Bedrohungen beschreibt und entsprechende Sicherheitsmaßnahmen vorsieht. Das vorliegende Dokument sollte bei der Erstellung eines solchen Konzepts berücksichtigt werden, kann dieses jedoch nicht ersetzen.

Abschließend wird hier noch auf weitere Quellen verwiesen, die – zum einen (Microsoft) aufgrund der eingesetzten Basistechnologie, zum anderen (BSI) aufgrund Vollständigkeit und Aktualität – wichtige Informationen zu relevanten Sicherheitsmaßnahmen beinhalten können:

- Windows Security Baselines von Microsoft https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-security-baselines
- Security Configuration Framework von Microsoft https://github.com/microsoft/SecCon-Framework/blob/master/windows-security-configuration-framework.md
- IT-Grundschutz-Kompendium des BSI https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html