8. Schutz vor Schadsoftware (Viren, Trojaner und Co.)

Bei den heutigen Bedrohungen in der Cyber-Security ist es unumgänglich, einen Rundumschutz für die firmeneigene IT zu implementieren.

Cyber-Attacken sind heute so fortschrittlich und auf Personen und Unternehmen (egal welcher Größe) zugeschnitten, dass ein wohl durchdachtes, aber einfach zu administrierendes System aus Endpoint-Sicherheit und Firewall von Nöten ist, welches Attacken schnell erkennt, stoppt und bereinigt - und das automatisiert.

Um einen Endpoint (Laptop, PC, Server, Smartphone, Tablet) abzusichern reicht ein einfacher Antivirenschutz bei weitem nicht mehr aus. Heutzutage sollte ein professioneller Endpoint-Schutz installiert werden, bestehend aus dem klassischen Antivirenschutz (Schutz vor typischer signaturbasierter Malware), und einem Schutz vor der heutigen am meist verbreiteten Bedrohung durch Ransomware (bösartige Verschlüsselung von Daten und Festplatten; Daten-Diebstahl zum Erzwingen von Zahlungen, um Daten wieder entschlüsseln zu können. Die größte Bedrohung durch Ransomware ist vor allem der Diebstahl von Daten und deren Weitergabe an Dritte, die es zu verhindern gilt. Gerade im Zuge der DSGVO ist darauf ein großes Augenmerk zu richten.

Dabei ist es erforderlich, dass die sogenannte Anti-Ransomware nicht nur eine ungewollte Verschlüsselung schnell erkennt und stoppt, sondern auch bereits verschlüsselte Daten wiederherstellen kann und eine automatische Bereinigung erfolgt. Des Weiteren muss der Diebstahl von Daten verhindert werden. Dies sollte über Standard-Richtlinien in der Software des Herstellers bereits definiert sein, um keinen größeren administrativen Aufwand betreiben zu müssen.

Des Weiteren sollte das Endpoint-Security-Produkt fähig sein, mittels eines „Security-Heartbeats“ mit der Firewall zu kommunizieren, um den Gesundheitsstatus des entsprechenden Endgerätes mitzuteilen. Im Falle einer Infektion kann die Firewall das Endgerät dann umgehend automatisiert in Quarantäne stellen, um eine Verbreitung der Cyber-Attacke auf andere Geräte zu verhindern.
Die Möglichkeit einer forensischen Untersuchung reaktiv oder auch proaktiv sollte gegeben sein um jederzeit über den Status der IT-Umgebung einen Bericht liefern zu können und um die Compliance nachweisen zu können.

Nach der automatischen Bereinigung des Endgerätes, sollte die Firewall über den „Security Heartbeat“ darüber informiert werden, um dann das Endgerät automatisiert wieder aus der Quarantäne nehmen zu können.

Von Vorteil ist, wenn alle Produkte über nur eine Konsole gemanagt werden können, um den administrativen Aufwand möglichst klein zu halten.

8.1 Firewall

Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Weiter gefasst ist eine Firewall auch ein Teilaspekt eines Sicherheitskonzepts.

So wie „Brandschutz“ ein Bündel von Maßnahmen ist (und nicht allein der Rauchmelder im Treppenhaus), kann dieser Teilaspekt je nach Sicherheitskonzept ein Bündel mehrerer Maßnahmen sein. Die Firewall kann aus mehreren Komponenten bestehen, von denen einige beispielsweise eine DMZ (DMZ = Demilitarisierte Zone, siehe Kap. 13 Begrifflichkeiten) versorgen. Ebenso kann die Wartung ein fester Bestandteil des Teilaspekts sein, genauso wie die Auswertung der Protokollierung von Firewallkomponenten.

Jedes Firewall-Sicherungssystem basiert auf einer Softwarekomponente. Die Firewall-Software dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender oder Ziel und genutzten Diensten. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand

festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden.

Abhängig davon, wo die Firewall-Software installiert ist, wird unterschieden zwischen einer Personal-Firewall (auch Desktop-Firewall) und einer externen Firewall (auch Netzwerk- oder Hardware-Firewall genannt). In Abgrenzung zur Personal-Firewall arbeitet die Software einer externen Firewall nicht auf dem zu schützenden System selbst, sondern auf einem separaten Gerät, das Netzwerke oder Netzsegmente miteinander verbindet und dank der Firewall-Software gleichzeitig den Zugriff zwischen den Netzen beschränkt. In diesem Fall kann „Firewall“ auch als Bezeichnung für das Gesamtsystem stehen (ein Gerät mit der beschriebenen Funktion). Bauartbedingt gibt es große konzeptionelle Unterschiede zwischen den beiden Arten.

Die Funktion einer Firewall besteht nicht darin, Angriffe zu erkennen. Sie soll ausschließlich Regeln für die Netzwerkkommunikation umsetzen.
Eine Firewall dient dazu, ungewollte Zugriffe auf Netzwerkdienste zu unterbinden. Sie orientiert sich dabei an den Adressen der Kommunikationspartner (also „wer darf worauf zugreifen“). In der Regel kann eine Firewall nicht die Ausnutzung einer Sicherheitslücke in dem Netzwerkdienst verhindern, wenn der Kommunikationspartner darauf zugreifen darf.

Bei der Ausnutzung des Rückwegs kann eine Firewall nicht vor dem Zugriff auf Sicherheitslücken des Browsers schützen, wenn der Kommunikationspartner auf die gefährdeten Bereiche des Programms zugreifen kann. Daher sollten Programme, die für den Netzwerkzugriff bestimmt sind, auf dem aktuellen Stand gehalten werden, um bekannte Sicherheitslücken dort zu schließen. Einige Firewalls bieten Filter an, die den Fernzugriff auf den genutzten Netzwerkdienst weiter einschränken, indem beispielsweise die Filterung von gefährdeten ActiveX-Objekten aus Webseiten vorgenommen wird. Der Browser kann dann auf solche in einer Webseite eingebetteten Objekte nicht mehr zugreifen (er zeigt sie nicht an), was gleichzeitig bedeutet, dass er über diese Objekte nicht angegriffen werden kann. Alternativ dazu lässt sich dieses Verhalten auch über die Konfiguration des verwendeten Browsers erreichen.

Je nach Firewall-Typ kann eine Firewall im günstigsten Fall auf den Netzwerkzugriff einer heimlich installierten Schadsoftware aufmerksam machen und mitunter sogar deren Netzwerkzugriff unterbinden. Ein solcher Erfolg ist allerdings stark von dem Geschick der jeweiligen Schadsoftware abhängig. Die Ausnutzung von Fehlern in der Netzwerkimplementierung des Betriebssystems kann eine Firewall im günstigsten Fall abwehren.

Erst wenn bekannt ist, gegenüber welchen Szenarien ein bestimmtes Maß an Sicherheit erreicht werden soll, kann man sich Gedanken über die Art und Weise machen, wie dies umgesetzt wird. Dabei hilft die Erstellung eines Sicherheitskonzepts. In größeren Organisationen kommt dafür üblicherweise eine eigene Sicherheitsrichtlinie zum Einsatz.

Welche Sicherheitseinstellungen eine Firewall bietet und wie diese konfiguriert werden, hängt vom jeweiligen Hersteller und Produkt ab. Neben fundierten Kenntnissen über digitale Netze ist deshalb auch unter Umständen eine Schulung, speziell zu den verwendeten Produkten nötig, damit „der Errichter“ die verantwortlichen Personen ihre Arbeit ordnungsgemäß ausführen können.

8.2 Virenscanner und Virenschutz

Ein Computervirus ist ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme, einen Bootsektor oder den RAM einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion.

Einmal gestartet, kann es Veränderungen am Betriebssystem oder an weiterer Software vornehmen (Schadfunktion), mittelbar auch zu Schäden an der Hardware führen. Als typische Auswirkung sind Datenverluste möglich. Computerviren beeinträchtigen die Computersicherheit und zählen zur Malware.

Der Ausdruck Computervirus wird umgangssprachlich auch für Computerwürmer und Trojanische Pferde genutzt, da es oft Mischformen gibt und für Anwender der Unterschied kaum zu erkennen ist.
Wie sein biologisches Vorbild benutzt ein Computervirus die Ressourcen seines Wirtcomputers und schadet ihm dabei häufig. Auch vermehrt es sich meist unkontrolliert. Durch vom Virenautor eingebaute Schadfunktionen oder durch Fehler im Virus kann das Virus das Wirtsystem oder dessen Programme auf verschiedene Weisen beeinträchtigen, von harmloseren Störungen oder Datenverlust bis zu Hardwareschäden.

Viren sind oft in einem Wirtprogramm eingebettet. Wird dieses Wirtprogramm aufgerufen, wird das Virus ausgeführt und kann sich weiterverbreiten.

Heutzutage sind Computerviren fast vollständig von Würmern verdrängt worden, da fast jeder Rechner an das Internet oder lokale Netze angeschlossen ist und die aktive Verbreitungsstrategie der Würmer in kürzerer Zeit eine größere Verbreitung ermöglicht.

Das verwendete Betriebssystem hat großen Einfluss darauf, wie hoch die Wahrscheinlichkeit einer Virusinfektion ist oder wie hoch die Wahrscheinlichkeit für eine systemweite Infektion ist. Grundsätzlich sind alle Betriebssysteme anfällig, die einem Programm erlauben, eine andere Datei zu manipulieren. Ob Sicherheitssysteme wie beispielsweise Benutzerrechtesysteme vorhanden sind und verwendet werden, beeinflusst, inwieweit sich ein Virus auf einem System ausbreiten kann.
Daher sollten Betriebssysteme immer mit den aktuellen Upgrades versehen werden.

Anwender sollten niemals unbekannte Dateien oder Programme aus unsicherer Quelle ausführen und generell beim Öffnen von Dateien Vorsicht walten lassen. Das gilt insbesondere für Dateien, die per E-Mail empfangen wurden. Solche Dateien – auch harmlos erscheinende Dokumente wie Bilder oder PDF-Dokumente – können durch Sicherheitslücken in den damit verknüpften Anwendungen auf verschiedene Weise Schadprogramme aktivieren. Daher ist deren Überprüfung mit einem aktuellen Antivirenprogramm Pflicht.

Antivirenprogramme schützen im Wesentlichen nur vor bekannten Viren. Daher ist es bei der Benutzung eines solchen Programms wichtig, regelmäßig die von den Herstellern bereitgestellten aktualisierten Virensignaturen einzuspielen. Viren der nächsten Generation (Tarnkappenviren) können von Antivirensoftware fast nicht mehr erkannt werden.

Mit Hilfe dieser Programme werden Festplatte und Arbeitsspeicher nach schädlichen Programmen durchsucht. Antivirenprogramme bieten meist zwei Betriebsmodi: einen manuellen, bei dem das Antivirenprogramm erst auf Aufforderung des Benutzers alle Dateien einmalig überprüft (on demand) und einen automatischen, bei dem alle Schreib- und Lesezugriffe auf die Festplatte und teilweise auch auf den Arbeitsspeicher überprüft werden (on access). Es gibt Antivirenprogramme, die mehrere für das Scannen nach Viren verantwortliche Programmmodule (engines) nutzen. Wenn diese unabhängig voneinander suchen, steigt die Erkennungswahrscheinlichkeit.

Standard-Antivirenprogramme bieten nie vollständigen Schutz, da die Erkennungsrate selbst bei bekannten Viren nicht bei 100 % liegt. Unbekannte Viren können von den meisten dieser Programme anhand ihres Verhaltens entdeckt werden („Heuristik“); diese Funktionen arbeiten jedoch sehr unzuverlässig. Auch entdecken Antivirenprogramme Viren oft erst nach der Infektion und können das Virus unter Umständen nicht im normalen Betrieb entfernen.

Wie zuvor beschrieben überfordert das rasante Wachstum komplexer koordinierter Bedrohungen die Schutzmechanismen vieler Unternehmen zunehmend. Insellösungen können einzelne Elemente eines Angriffs stoppen. Sie arbeiten jedoch nicht zusammen, um Daten, Geräte und das Netzwerk vor raffinierten und koordinierten Cyber-Angriffen zu schützen. Gleichzeitig tun sich überlastete IT-Abteilungen zunehmend schwer, schnell genug auf diese Bedrohungen reagieren zu können.

Synchronized Security Systems sind Sicherheitssysteme (Virenscanner und Virenschutz), die es den Abwehrmaßnahmen ermöglichen, so koordiniert zu agieren wie die Angriffe, vor denen sie schützen. Diese Systeme kombinieren in der Regel eine intuitive Security-Plattform mit mehreren Softwarepaketen, die aktiv zusammenarbeiten. Dieser kombinierte Sicherheitsansatz schützt optimal gegen komplexe Bedrohungen.

Wichtig für einen guten Virenschutz sind folgende Punkte:

1. Schnelle Erkennung (Virenscan)
Hinweise auf hochentwickelte Bedrohungen (z. B. verdächtiger Netzwerkverkehr) werden sofort zwischen Firewall und Endpoint (PC, Desktop) ausgetauscht, um Angriffe zu erkennen und abzuwehren.

2. Einfache Analyse (Identifizieren)
Die Funktion zur aktiven Identifizierung kompromittierter Systeme tauscht Computernamen, Benutzer und Pfade zwischen Endpoints und Firewall aus, sodass schnell reagiert werden kann.

3. Weniger Beeinträchtigungen (Isolieren und Bereinigen)
Kompromittierte Endpoints werden von der Firewall automatisch isoliert und der Endpoint beendet und entfernt die Schadsoftware.

4. Automatische Reaktion
Sicherheitsinformationen werden über das gesamte System hinweg ausgetauscht und genutzt. Infizierte Endpoints werden isoliert, bevor die Bedrohung sich ausbreiten kann und die Reaktionszeit bei Sicherheitsvorfällen minimiert sich um 99,9 %.

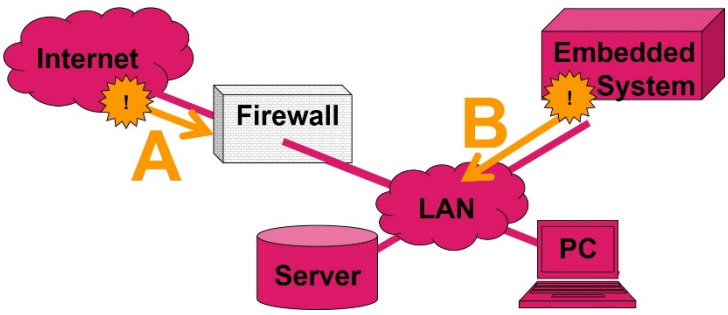
8.3 Cyber-Security bei Videoanlagen

8.3.1 Allgemeines

Digitalisierung und Vernetzung verändern auch die Videosicherheitstechnik grundlegend:
Klassische analoge Videokameras mit direkt zugeordneten (dedizierten) Videoaufzeichnungsgeräten (Recordern) werden ersetzt durch immer leistungsfähigere IP-Kameras, die in einer komplexen IT-Infrastruktur betrieben werden. Damit wachsen auch die Herausforderungen, die für einen sicheren Betrieb dieser Anlagen zu meistern sind.

Das Thema Sicherheit wird meist intuitiv mit Angriffen von außen in Verbindung gebracht. Folgerichtig unterliegen bei den üblichen Firewall-Einstellungen vor allem jene Verbindungen strengen Regeln, die von außen (aus dem Internet) nach innen (in das private Netz, LAN) aufgebaut werden. Hingegen wird der Aufbau von Verbindungen von innen nach außen meist nicht oder nur wenig reglementiert, um den Zugriff der Anwender auf die verschiedenen weltweiten Internet-Anwendungen und Dienste nicht zu beeinträchtigen.

Netze sind oft nur gegen Angriffe von **außen (A)** geschützt. Die Erfahrung zeigt jedoch, dass Angriffe auch von **innen (B)** erfolgen. Viele Videoanlagen sind dagegen unzureichend geschützt. Statt zu mehr Sicherheit führen solche Anlagen zu mehr Risiko. Hier besteht dringender Handlungsbedarf für Errichter und Betreiber.



8.3.2 Unterschätztes Risiko „Embedded Systems“

Embedded Systems (eingebettete Systeme) sind Computer, die für einen bestimmten technischen Zweck in ein Gerät eingebaut werden und dort – für den Anwender oft unsichtbar – ihren Dienst

tun. Mit Produkten aus dem Smart-Home-Bereich, „intelligenten“ Lautsprechern, Alarmanlagen und auch IP-Kameras halten sie Einzug in viele private Netze, ohne dass den Anwendern die damit verbundenen Gefahren bewusst sind.

Embedded Systems bergen Risiken, weil sie durch die Firewall von innen nach außen Verbindungen aufbauen können. Ist eine solche Verbindung erst einmal hergestellt, können Angreifer darüber das Gerät steuern und somit das private Netz (LAN) von innen angreifen.

Server und PCs sind als sicherheitsrelevante Technik klar zu erkennen und werden entsprechend sorgfältig in Sicherheitskonzepten berücksichtigt. Risiken, die von eingebetteten Systemen ausgehen, werden dagegen häufig unterschätzt, weil bei diesen Geräten die Hauptfunktion im Mittelpunkt steht und nicht auf den ersten Blick zu erkennen ist, was alles im Gehäuse steckt. Eine IP-Kamera ist aber eben nicht nur eine Kamera, sondern ein voll vernetzter Computer mit allen Möglichkeiten und Risiken, die diese komplexe Technik bietet.
Bei Entwicklung und Auswahl von embedded Systems stehen meist Funktion und Preis im Vordergrund. Das hat zur Folge, dass die Datensicherheit oft vernachlässigt wird.

Viele embedded Systems bauen bereits ab Werk automatisch Verbindungen zu externen Servern auf, etwa für Updates, Fernwartung oder zum Speichern von Daten in der „Cloud“. Diese Verbindungen unterlaufen die Firewall; der Anwender hat in der Regel keine Kontrolle darüber, welche Daten über diese Verbindungen transportiert werden. Bei manchen Geräten sind Hintertüren bekannt geworden, die versehentlich oder absichtlich eingebaut wurden. Mitunter werden Geräte auch gezielt von Geheimdiensten, Industriespionen oder der organisierten Kriminalität manipuliert. Solche kompromittierten Systeme stellen ein erhebliches Sicherheitsrisiko für das gesamte betroffene Netzwerk und Unternehmen dar.

Dieses Risiko ist nicht abstrakt und theoretisch, sondern ganz konkret und hat in der Praxis bereits zu erheblichem wirtschaftlichem Schaden geführt. Das zeigen folgende Beispiele:

- Eine russische Hackergruppe hat im Zuge der Kampagne „Carbanak“ u.a. Überwachungskameras in Banken kompromittiert und konnte Millionenbeträge erbeuten.
- Die Schadsoftware „Mirai“ hat u.a. zahlreiche Überwachungskameras für einen DDoS-Angriff genutzt.
- Überwachungskameras des amerikanischen Herstellers „NetBotz“ waren jahrelang mit einer Hintertür in vielen Unternehmen und kritischen Bereichen eingesetzt, u.a. in Serverräumen.

Auch aus Gründen der Informationssicherheit und des Datenschutzes müssen Errichter und Betreiber von Videosicherheitssystemen sicherstellen, dass nur berechtigte Nutzer auf die Geräte und Daten zugreifen können.

Mögliche Ursachen für Angriffe von innen:

- Von Anwendern eingebrachte Schadsoftware/Plugins
- Backdoors der Hersteller, z.B. für Support, Behörden, …
- Sicherheitslücken (fehlende Updates, Standard-Passworte)
- Verbindungen für Updates, Video-Hosting, Fernwartung, …)
- Für Spionagezwecke präparierte Geräte
- uvm.

8.3.3 Herausforderung IP

Für klassische Videosicherheitsanlagen hatte sich in der Vergangenheit die Abkürzung „CCTV“ etabliert. Aufgrund neuer weltweiter Normierung wurde aus „CCTV“ nun „VSS“. Das CC steht für