Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Sicherheit von IP-basierten Überwachungskameras

Netzwerkfähige Überwachungs- oder Webkameras sind – wie auch viele andere Ausprägungen von Geräten im Kontext des Internet der Dinge (Internet of Things, IoT) – ein potenzielles Sicherheitsrisiko. Dies ist insbesondere darin begründet, dass bei Entwicklung und Betrieb dieser Geräte der Aspekt der Cyber-Sicherheit ein nicht oder nur nachrangig beachtetes Entwurfsziel ist. Daher können solche Kameras zum Sicherheitsrisiko für die eigene Infrastruktur sowie für Dritte werden.

In den vergangenen Jahren ist es immer wieder zu Vorfällen im Zusammenhang mit vernetzten bzw. IP-basierten Überwachungskameras gekommen, z. B.:

- 2013: Eine russische Hackergruppe kompromittiert im Zuge der Kampagne "Carbanak" mehrere Banken in verschiedenen Ländern und erbeutet einen dreistelligen Millionenbetrag. Bei diesen Angriffen wurden Überwachungskameras innerhalb der Finanzinstitute kompromittiert, um Bildschirminhalte und Tastatureingaben auszuspähen, Mitarbeiter z. B. über Namensschilder/Mitarbeiterausweise als Ziel für Spear-Phishing zu identifizieren sowie Gewohnheiten und Reaktionen der Mitarbeiter in Erfahrung zu bringen.[1]
- 2014: Die Webseite Insecam stellt die Videobilder bzw. -streams von 73.000 unzureichend geschützten Webcams (maßgeblich aus dem privaten Anwendungsbereich) offen zur Verfügung.[2]
- 2015: Die Schadsoftware Conficker aus dem Jahr 2008 infiziert eine Vielzahl von Bodycams verschiedener Polizeien.[3]
- 2016: Eine große Anzahl von durch die Schadsoftware Mirai kompromittierten Überwachungs-/Webkameras wird dazu verwendet, um einen der massivsten DDoS-Angriffe der Geschichte auf den Fachjournalisten Bryan Krebs durchzuführen.[4]

Ziel dieses Dokuments ist es, einen Überblick über die elementaren Best Practices zum sicheren Betrieb solcher Kameras zu geben.

1 http://newsroom.kaspersky.eu/de/texte/detail/article/der-grosse-bankraub-cybergang-carbanak-stiehlt-eine-milliarde-us-dollar-von-100-finanzinstitu
2 http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html
3 http://www.goipower.com/?pageId=40
4 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

1 Produktauswahl und Beschaffung

Schon bei der Produktwahl sollten nicht nur das Preis-Leistungs-Verhältnis betrachtet werden, sondern auch Aspekte der IT-Sicherheit. Hier spielt vor allem die angebotene Funktionalität des Produktes und die Gewährleistungen des Herstellers eine wichtige Rolle. Grundsätzlich ist von der Verwendung von Kameras mit einem Cloud-Konzept abzuraten. In diesem Falle fließen sensible Daten über Dritte (z. B. Kamerahersteller) und werden dort für einen Zugriff über das Internet gespeichert. Auch die Verwendung von Wi-Fi/WLAN – insbesondere in kritischen Einsatzbereichen – sollte vermieden werden, sofern dies die Einsatzbedingungen erlauben.

Ein grundlegendes Ziel zum sicheren Einsatz von IP-Kameras ist die Minimierung der Angriffsfläche. Um diese von Beginn an gering zu halten, empfiehlt es sich, Kameras zu beschaffen, die nur die für den konkreten Einsatzzweck erforderlichen Dienste/Ports implementieren. Alternativ sollte es möglich sein, nicht benötigte Dienste zu deaktivieren. Ist auch dies nicht möglich, müssen entsprechende Einschränkungen bei der Inbetriebnahme auf Netzwerkebene (z. B. Firewall) vorgenommen werden, um die Verwendung von nicht benötigten Diensten zu verhindern.

Um eine vertrauliche Übertragung von Video- und Konfigurationsdaten zu gewährleisten, sollte das Produkt ein auf Verschlüsselung basierendes Protokoll (z. B. SSL/TLS bzw. SSH) unterstützten. Bietet das Produkt selbst keine Verschlüsselung, muss dies bei der Inbetriebnahme, z. B. Über ein Virtual Private Network (VPN), flankierend umgesetzt werden.

Sofern der Einsatzzweck dies erfordert, sollten die Kameras ein differenziertes Rollen-/Rechtekonzept für unterschiedliche Benutzer bereitstellen.

Weiterhin muss der Hersteller für einen hinreichend langen Zeitraum die Bereitstellung von Patches bzw. Updates gewährleisten. Dies wird meist mit End Of Service (EOS) beschrieben – nicht zu verwechseln mit End Of Life (EOL), was das Ende der Herstellung und des Verkaufs eines Produktes bezeichnet.

2 Installation und Inbetriebnahme

Nicht nur bei der Beschaffung, sondern auch bei der Inbetriebnahme von IP-Kameras existieren Empfehlungen zum sicheren Einsatz. Grundsätzlich gilt: Embedded Webserver, wie beispielsweise bei Überwachungskameras, sind typischerweise nicht dazu geeignet, um über das Internet unbeschränkt erreichbar gemacht zu werden.

Während der erstmaligen Konfiguration der Kamera sollten hinreichend sicherer Passwörter verwendet werden. Zusätzlich empfiehlt sich die Verwendung von alternativen Authentisierungsmechanismen, wie z. B. zertifikatsbasierter Authentisierung oder Multi-Faktor Authentisierung. Weiterhin sollten in diesem Schritt nicht benötigte Dienste der Kamera deaktiviert werden. Dies gilt insbesondere für chronisch unsichere Dienste, wie z. B. Telnet oder SNMPv1/v2.

Um den Zugriff der IP-Kameras auf ein Minimum zu beschränken, sollten mittels einer Firewall nur zuvor definierte ein- und ausgehende Verbindungen erlaubt werden.

Für ausgehende Verbindungen sollten die validen Ziele einer Verbindung, wie z. B. Update-Server des Herstellers, Speicherort der Videodaten und Managementsystem, konfiguriert werden. Ob und wie die Kameras die Server des Herstellers kontaktieren müssen, um die Verfügbarkeit von Updates zu prüfen, sollte in der Produktdokumentation recherchiert werden.

Vermeiden Sie möglichst eine Konfiguration im Router, bei der die Kamera eine Verbindung nach außen aufbauen kann.

Sollte eine Erreichbarkeit der Kameras von außen (d. h. aus dem Internet eingehend) erforderlich sein, so sollte dies nur mit hinreichender Authentisierung erfolgen.

Vermeiden Sie möglichst die Freigabe von extern eingehenden Verbindungen im Router.

Geben Sie in keinem Fall im Router den Zugriff über Telnet (Port 23) von außen frei. Nutzen Sie nach außen hin nicht einen der standardmäßig verwendeten Ports (23, 1023, 2323) sondern einen Zufallswert im Bereich 10000 bis 65535.

Geben Sie im Router den Zugriff über SSH (Port 22) nur frei, wenn dieser mit hinreichend sicheren individuellen Passwörtern geschützt ist. Eine höhere Sicherheit erlangen Sie, wenn der Zugriff nicht über Benutzername und Passwort, sondern durch ein Softwarezertifikat gesichert wird. Nutzen Sie nach außen hin nicht einen der standardmäßig verwendeten Ports (22, 1022, 2222) sondern einen Zufallswert im Bereich 10000 bis 65535.

Gegebenenfalls kann der Zugriff zusätzlich durch die Verwendung von VPN weiter abgesichert werden. Bei der Verwendung von VPN ist darauf zu achten, dass ausreichend starke kryptografische Verfahren und entsprechende Schlüssellängen verwendet werden.

Es empfiehlt sich auch, die Kameras in einem separaten physischen Netzbereich bzw. innerhalb eines separaten Virtual Local Area Networks (VLANs) zu betreiben, um ein laterales Ausbreiten bei einer Kompromittierung der Kameras zu vermeiden.

Abhängig vom Einsatzort der Kameras sollte ein physikalischer Zugriffsschutz umgesetzt werden. Dieser schützt nicht nur vor Vandalismus, sondern auch vor einer Veränderung der Konfiguration, die häufig durch das Zurücksetzen auf den Werkszustand ermöglicht wird.

3 Betriebsphase

Während des Betriebes der Überwachungskameras sollte regelmäßig überprüft werden, ob neue Updates/Patches zur Installation zur Verfügung stehen. Zusätzlich zur Firmware der Kameras sollten auch Drittkomponenten, wie z. B. Administrations- oder Managementsoftware, auf Aktualität überprüft werden. Falls neue Updates verfügbar sind, sind diese zeitnah einzuspielen.

Es empfiehlt sich, die Kommunikation (ein- und ausgehende Verbindungen) regelmäßig auf Auffälligkeiten zu kontrollieren. Hierbei können Logfiles von Firewalls genaue Informationen liefern, mit wem die Kamera über welchen Dienst kommunizieren möchte und ob diese Verbindungen erlaubt oder blockiert wurden. Weiterhin können auch die Kameras oder die dazugehörige Administrations- oder Managementsoftware Informationen liefern, ob die Kamera erwartungsgemäß verwendet wird.

Aktuelle Schadsoftware auf Überwachungskameras und anderen IoT-Geräten arbeitet oftmals nur im Hauptspeicher, statt sich persistent im System einzunisten. Daher ist ein regelmäßiger Neustart solcher Kameras ratsam. Dies kann eine Infektion bereinigen, wenngleich es nicht vor einer Neuinfektion schützt.

4 Zusammenfassung der Maßnahmen

- Cloud-Konzepte vermeiden
- Wi-Fi/WLAN vermeiden
- Allgemeine Erreichbarkeit über das Internet vermeiden
- Nur benötigte Dienste aktivieren
- Nur verschlüsselt kommunizieren
- Beachtung des EOS Zeitraums
- Einsatz ausreichend starker Authentisierungsmechanismen
- Hinreichende starke Passwörter wählen
- Kommunikation durch Firewallregeln beschränken
- Netzwerkseparation einsetzen
- Fernzugriff nur über VPN ermöglichen
- Zeitnahes Einspielen von Updates
- Monitoring der Kommunikation (Logfiles)
- Optionale Verwendung von Rechte- und Rollenkonzepte
- Optional Verwendung physikalischer Zugriffsschutz

5 Weitere Informationen

Die folgenden Empfehlungen der Allianz für Cyber-Sicherheit liefern zusätzliche Informationen und beschreiben Umsetzungsempfehlungen von zuvor genannten Maßnahmen:

- Anforderungen an netzwerkfähige Industriekomponenten[5]

  Diese Empfehlung ist neben netzwerkfähigen Industriekomponenten auch auf eine Vielzahl von IoT-Geräten anwendbar. Hierin werden insbesondere auch Anforderungen an den Hersteller bzw. Integrator beschrieben.

- Sichere Passwörter in Embedded Devices v1.0[6]

  Diese Empfehlung beschreibt das allgemeine Problem von festcodierten Zugangsdaten in Embedded Devices, zu denen auch Überwachungskameras zählen. Es werden hier Empfehlungen für Hersteller, Integratoren und Betreiber gegeben.

- Rohde & Schwarz SIT GmbH: Checkliste Netzwerksicherheit[7]

  Diese Empfehlung beschreibt, wie der Netzübergang in das Internet abgesichert werden kann und gibt Empfehlungen, wie ein Netzwerk z. B. durch VLANs segmentiert werden kann.

5 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_067.pdf
6 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_069.pdf
7 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/Partnerbeitrag_Rohde-Schwarz.html

Aus dem IT-Grundschutz ist insbesondere der Baustein B3.407 „Eingebettetes System“ anzuwenden. Darüber hinaus liefern die folgenden Maßnahmen aus dem IT-Grundschutz weitere Informationen und beschreiben Umsetzungsempfehlungen von zuvor genannten Maßnahmen:

- B 3.407 Eingebettetes System[8]
- M 2.8 Vergabe von Zugriffsrechten[9]
- M 2.11 Regelung des Passwortgebrauchs[10]
- M 2.109 Rechtevergabe für den Fernzugriff[11]
- M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates[12]
- M 2.417 Planung der technischen VPN-Realisierung[13]
- M 2.555 Entwicklung eines Authentisierungskonzeptes für Anwendungen[14]
- M 4.7 Änderung voreingestellter Passwörter[15]
- M 4.488 Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen[16]
- M 5.61 Geeignete physische Segmentierung[17]
- M 5.62 Geeignete logische Segmentierung[18]
- M 5.77 Bildung von Teilnetzen[19]

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

8 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03407.html?nn=6604938
9 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02008.html
10 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html
11 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02109.html
12 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02273.html
13 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02417.html
14 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02555.html
15 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04007.html
16 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04488.html
17 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05061.html
18 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05062.html
19 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05077.html