IP-Videoüberwachungskameras unwissentlich für DDoS-Attacken missbraucht – Tipps&Tricks zum Schutz der Sicherheitstechnik

Von Lutz Rossa

Von Botnetzen ausgehende DDoS-Attacken (DDoS: Distributed Denial of Service) waren nicht nur im vergangenen Jahr des Öfteren in den Schlagzeilen. Verteilte Angriffe auf Ziele wie Amazon, Twitter, Spotify usw. wurden in der Absicht durchgeführt, diese einer Dienstblockade zu unterziehen – Unternehmen also funktionsunfähig zu machen. Das Besondere daran war, dass die Botnetze nicht aus herkömmlichen gekaperten Rechnern bestanden, sondern aus IP-Videoüberwachungskameras. Deren Speicher- und Rechenleistung ließ man für sich arbeiten. Es wurden also mit den Sicherheitssystemen ausgerechnet eben jene Technik zu kriminellen Taten zweckentfremdet, die für Safety und Security sorgen soll.

Die Hersteller reagieren –Sicherheitslücken in Videokameras schließen

Auf die missbräuchliche Nutzungsmöglichkeit insbesondere von IP-Videokameras haben viele Hersteller nun reagiert. So hat Geutebrück seine Kunden informiert, wie Sicherheitslücken in seinen Topline-Kameras geschlossen werden können. Hier war es sehr einfach, durch Änderung des Standardpassworts in ein individuelles Passwort sowie dem Setzen eines Hakens, anonymen Nutzern den Zugriff auf die Kamera nicht zu gestatten. Axis geht einen Schritt weiter und hat nun seine „Camera Management Softwareplattform“ zu einem „Device Manager“ weiterentwickelt. Dieser soll nun den „proaktiven Schutz der Geräte und Netzwerke erleichtern“. So können laut Hersteller Wiederherstellungspunkte und werkseitige Standardeinstellungen konfiguriert, die Gerätefirmware aktualisiert und Benutzerkonten mit Kennwörtern verwaltet und aktualisiert werden. Zudem soll es möglich sein, 802.1X-Zertifikate für Authentisierungs- und Verschlüsselungsmechanismen (HTTPS, TLS/SSL) zu verwalten. Mobotix hat ebenfalls auf die Angriffe reagiert und gemeinsam mit einem auf Cyber Security spezialisierten Partner im Rahmen des „Cactus Concept“ einen „Leitfaden zur optimalen Absicherung Ihres Mobotix Videosystems“ sowie ein Whitepaper zu der Thematik Cyber Security herausgebracht. Der Leitfaden kann als Hilfestellung insbesondere zur sicheren Konfiguration der Kameras genutzt werden. Darüber hinausgehende Maßnahmen, die das Netzwerk selbst sowie das Backend mit Videomanagementsoftware, Speicherung, Verwaltung usw. betreffen, sind darin nicht aufgeführt. HIKVISION hat seine Kameras dahingehend konfiguriert, dass bei Inbetriebnahme ein individuelles Passwort konfiguriert werden muss. Telnet hat man grundsätzlich deaktiviert.

Das können Sie in Ihrem Unternehmen machen

1. Schützen Sie Ihre Sicherheitstechnik auch durch informationstechnische Standardmaßnahmen. Bisher betrachteten die Unternehmen zumeist den Schutz auf baulicher, sicherheitstechnischer und organisatorischer Ebene. Doch diese Schutzmaßnahmen sind nur dann genügend wirksam, wenn man die Systeme zur Sicherung auch in informationstechnischer Sicht, analog zur Office- und Produktions-IT, entsprechend härtet.

2. Legen Sie für alle Netzwerkdienste dieselben Kriterien an. Netzwerke sind in der Regel dienstneutral. Dem Videosystem wird nicht immer ein dediziertes Netz bereitgestellt. Angreifbare Kameras befinden sich somit möglicherweise innerhalb des Produktionsnetzes und kompromittieren dieses bereits durch unsichere Konfiguration. Somit sind Maßnahmen zur Sicherstellung der Informationssicherheit auch für die Sicherheitstechnik zu berücksichtigen.

3. Überprüfen Sie Ihre IP-fähige Sicherheitstechnik auf eine sichere Konfiguration. Fangen Sie bei einfachen Dingen wie der Zugangssicherung (Passworte), z. B. der Videokameras, an und laufen Sie sozusagen über das Netzwerk bis zur Absicherung der Server, Clients und der darauf laufenden Anwendungssoftware.

4. Sorgen Sie für ein ausreichendes Sicherheitsbewusstsein bei Ihren Mitarbeitern. Für einen sicheren Schutz vor Fremdzugriff und funktionierende Authentisierungsmechanismen müssen auch die Mitarbeiter eine ausreichende Sensibilität aufweisen. Für eine so triviale Maßnahme wie die Änderung eines Standardpassworts in ein individuelles Passwort sind weder Informatikstudium noch tiefergehende Kenntnisse der Videotechnik erforderlich. Der normale Menschenverstand reichte hier völlig aus. Aber man muss wissen, dass hier Lücken zu schließen sind. Das bedeutet: Awareness!

5. Testen Sie die Sicherheit Ihrer IT-Systeme in regelmäßigen Abständen. Zur Nachweisführung einer erfolgreichen Umsetzung sind, analog zu Härtetests bei der TGA-Infrastruktur und Gebäudeautomation, Penetrationstests empfehlenswert, also gezielte Angriffe auf die IT-Systeme.

6. Tragen Sie Ihre Forderungen zur Umsetzung von Maßnahmen zur Informationssicherheit an die zuständigen Errichterfirmen heran. Die von den anfangs genannten Herstellern durchgeführten Konfigurationsänderungen dürfen nur ein Teil der Härtung sein. Im Rahmen von Neuerrichtungen, aber auch im Zuge der turnusmäßigen Wartung, sollten die IT- und Netzwerk-Verantwortlichen in Unternehmen zusammen mit den zuständigen Errichterfirmen gemeinsam z. B. unter Zuhilfenahme der ISO 27001 ff. die gesamte Sicherheitstechnik härten und somit vor Missbrauch und Angriffen schützen.

Über den Autor

Rossa, Lutz, Dipl.-Ing. (FH). Planer und Berater der VON ZUR MÜHLEN`SCHE GmbH, Sicherheitsberatung – Sicherheitsplanung – Rechenzentrumsplanung, BdSI, Bonn. ISMS ISO 27001 Lead Auditor. Tätigkeitsbereich: Planung, Beratung Sicherheitszentralen und Leitzentralen, sicherheitstechnische Planung. Er ist zudem Referent auf dem neuen SIMEDIA-Fachforum „Security over IP“.