» Erfolgskritische Faktoren

Woran Sie vertrauenswürdige Anbieter in Sachen Cybersicherheit erkennen

Viele Ereignisse in der letzten Zeit haben das Thema Cybersicherheit für Unternehmen wieder verstärkt in den Mittelpunkt gerückt. Cyber-Kriminelle haben versucht, von den Auswirkungen der Pandemie und der sprunghaft gestiegenen Arbeit im Homeoffice zu profitieren.

In Europa gab es im Jahr 2020 304 Angriffe von außergewöhnlicher Bedeutung, mehr als doppelt so viele wie im Jahr 2019. Dazu kommt nun noch das erhöhte Risiko der Cyberkriegsführung im Zuge des russischen Krieges gegen die Ukraine. John Edwards, „Information Commissioner" der britischen Regierung, äußerte beispielsweise, dass wir uns seiner Ansicht nach in einer neuen Ära der Sicherheit befinden

„Der menschliche Faktor ist oft Einfallstor für Angriffe."

und Unternehmen ihre Wachsamkeit gegenüber staatlich unterstützen Hackern deutlich erhöhen müssen.

Kameras als Ziel von Angriffen

Der zunehmende Einsatz von vernetzten Geräten wie IP-Kameras und Sensoren des „Internet of Things" (IoT) bietet Hackern mehr Möglichkeiten, Schäden zu verursachen. Kameras der aktuellen Generation sind technisch weit entwickelt und verfügen über die neueste Firmware. Ältere Geräte müssen jedoch zwingend auf dem neuesten Stand gehalten werden, wenn sie keine Einfallstore für Hackerdarstellen sollen.

Leider investieren viele Unternehmen zwar in ihre physischen Sicherheitssysteme, unterschätzen aber die Gefahr, dass Videoüberwachungs- und IoT-Geräte von kriminellen Akteuren als „backdoors" genutzt werden können. Kompromittierte Kameras und andere angeschlossene Hardware können zum Ausgangspunkt für Angriffe auf ein Netzwerk werden – diese Technik wird auch als „Pivoting" bezeichnet. Hacker erhalten so Zugriff auf vertrauliche Informationen und nutzen diese, um Personen oder Unternehmen zu erpressen bzw. Daten zu stehlen.

Verantwortungsbewusste Produzenten von Kameras setzen auf Technologie (Hard- und Software), Schulungen, Zusammenarbeit mit Kunden und objektive Zertifizierungen, die das Sicherheitsniveau ihrer Prozesse und Lösungen dokumentieren, um das Problem anzugehen. Es gibt dabei einige klare Kriterien, die den entscheidenden Unterschied für die Cybersicherheit Ihres Überwachungssystems ausmachen können:

NDAA-Konformität

Der "National Defense Authorization Act 2019 (NDAA)" ist ein guter Ausgangspunkt. Dieses US-Bundesgesetz verbietet Bundesbehörden und ihren Auftragnehmern die Nutzung von Videoüberwachungslösungen verschiedener Unternehmen. Ein Dienstleister, der NDAA-konform ist, erfüllt also alle erforderlichen Standards für US-Bundesbehörden – dies bedeutet ein sehr hohes Maß an Sicherheit und Verlässlichkeit, das Vertrauen bei sämtlichen Organisationen und Regierungsstellen schafft. Hanwha Techwin bestätigt die NDAA-Konformität seines gesamten Produktportfolios und verpflichtet sich, alle staatlichen und internationalen Handelsvorschriften einzuhalten. Übrigens verdichten sich die Anzeichen, dass europäische Regierungen die Umsetzung ähnlicher Gesetze erwägen.

Hersteller, die ihre Produkte von Beginn an mit Blick auf Cybersicherheit entwickeln, erkennen Sie an Zertifizierungen wie dem „UL Cybersecurity Assurance Program" (UL CAP). Diese Anbieter produzieren stabile und sichere Systeme, die regelmäßig gewartet sowie gepatcht werden und beseitigen Schwachstellen so proaktiv. Hanwha Techwin gehört zu den wenigen Herstellern in der Videoüberwachungsbranche, die diese „UL CAP-Zertifizierung" für ihre Produkte erhalten haben. „Secure by Default" ist eine weitere wichtige Zertifizierung, die dokumentiert, dass ein Produkt standardmäßig cyber- und netzwerksicher ist und kein weiteres Härten der Systemsicherheit nötig macht.

Sie sollten zudem auf eine ISO 27001-Zertifizierung Ihrer Lieferanten achten. Diese zu erhalten und zu bestätigen, ist für Anbieter durchaus anspruchsvoll, da sie kontinuierliche Optimierung erfordert. Sie ist dadurch aber eine Garantie, dass ein Dienstleister die Informationssicherheit mit größter Sorgfalt behandelt. Hanwha Techwin ist nach ISO27001 zertifiziert.

Uri Guterman, Head of Product & Marketing, Hanwha Techwin Europe

Schnelle Reaktion auf neue Sicherheitsrisiken

Welchen Grad an Sicherheit Kameras eines Herstellers jetzt und zukünftig bieten, lässt sich am Forschungsaufwand erkennen, den dieser in die Identifikation neuer Bedrohungen investiert. Wenn eine Sicherheitslücke entdeckt wird, ist eine schnelle Reaktion absolut entscheidend. Wer die entsprechenden Ressourcen bereitstellt, kann schneller gegen Bedrohungen der Cybersicherheit vorgehen. Das S-CERT-Team (Security Vulnerability ResponseCenter) von Hanwha Techwin ist einzigartig in der Branche. Die Spezialisten arbeiten ausschließlich an der Entwicklung proaktiver Schutzmaßnahmen gegen unbefugten Gerätezugriff sowie der sofortigen Behebung von Sicherheitsschwachstellen.

Cybersecurity-Schulungen

Die sichersten Anbieter schulen ihre Netzwerkpartner, also vor allem die Nutzer der Produkte und die Techniker, um sicherzustellen, dass Software und Hardware immer aktualisiert werden, um neue Bedrohungen zu bekämpfen. Die gesamte Hardware muss stets mit der neuesten Firmware und den neuesten Sicherheits-Patches aktualisiert werden.

Der menschliche Faktor ist ebenfalls oft Einfallstor für Angriffe. Hier bieten verantwortungsbewusste Anbieter Schulungen und Leitfäden, wie Kunden ein System sicher halten und Social-Engineering-Angriffe wie beispielsweise Phishing vermeiden können.

Fehler haben Konsequenzen

Für alle Organisationen steht viel auf dem Spiel, insbesondere wenn ihre Kameras sensible, personenbezogene Daten erfassen. Die Kosten einer Datenschutzverletzung sind immens (durchschnittlich 4,24 Millionen US-Dollar pro Verletzung im Jahr 2021 – der höchste Wert seit 17 Jahren). Auch der Reputationsschaden für das Unternehmen und der Vertrauensverlust können massive Folgen haben. Stéphane Nappo, Chief Information Security Officer der französischen Bank Société Générale, sagte dazu: "Es dauert 20 Jahre, um einen Ruf aufzubauen und ein paar Minuten eines Cybervorfalls, um ihn zu ruinieren."

Echter Partner in Sachen Cybersicherheit

Daher ist es wichtig, mit Anbietern zusammenzuarbeiten, die Cybersicherheit ernst nehmen (und dies auch nachweisen können), die nötigen Ressourcen bereitstellen, um Bedrohungen schnell zu erkennen und die mit Kunden und Technikern zusammenarbeiten, um deren Kompetenz im Bereich Cybersicherheit zu unterstützen.

Wenn eine Sicherheitslücke entdeckt wird, ist eine schnelle Reaktion absolut entscheidend.

Obwohl kein System hundertprozentigen Schutz gegen Cybersecurity-Bedrohungen bietet, können Sie sich bei einer Zusammenarbeit mit Hanwha Techwin darauf verlassen, dass wir alles tun, um Schwachstellen schnell zu erkennen und zu eliminieren.

IP-Kameras sind heute der Standard, also muss die Videoüberwachungsbranche ihre Anstrengungen erhöhen, um Cyber-Risiken durch Technologie, Kompetenz und unabhängige Zertifizierungen zu minimieren.

www.hanwha-security.eu/de/