



Pressekontakt:

VdS warnt: Millionen Videokameras anfällig für Hacking

Gefährlicher Zugriff auf neun Millionen Videokameras: Genau die unsicheren Cloud-Funktionen, vor denen Polizei und VdS seit Jahren warnen, ermöglichen Manipulationen der Überwachungssysteme hunderter Endhersteller. // Präzise Hilfestellungen für den sicheren Fernzugriff finden Entwickler in den kostenlos erhältlichen Richtlinien VdS 3169.

Köln, 5. November 2018. Die Polizei und VdS warnen seit Jahren vor der oftmals leichten Angreifbarkeit unsicherer Cloud-Lösungen – selbst bei Komponenten, die im Sicherheitsbereich eingesetzt werden. Das jüngste Beispiel sind Videokamera-Bauteile eines der weltweit größten Hersteller hierfür (Sitz in Ostchina). Hack-Versuche der Wiener IT-Sicherheitsberater SEC Consult deckten schnelle Zugriffsmöglichkeiten für neun Millionen in Nutzung befindliche Kameras auf, davon 1,3 Millionen in Deutschland. Auch Programmmanipulationen waren leicht möglich.

Besonders problematisch ist, dass diese Komponenten zwar von mehr als hundert Endherstellern genutzt, aber meist nirgendwo ausgewiesen werden. Übrigens bezog das Botnet „Mirai“ (Täter gefasst und verurteilt), welches 2016 weite Teile des Internets inklusive Twitter, Spotify und Netflix lahmlegte, seine Angriffsstärke zu großen Teilen aus gehackten Komponenten eben dieses Herstellers.

Sebastian Brose, Leiter des VdS-Produktmanagements im Geschäftsbereich Produkte und Unternehmen, erklärt: „Optimierungen erfolgten seitdem meist nicht. Sehr viele für Kriminelle hochinteressante Institutionen auf der ganzen Welt nutzen die angreifbaren Komponenten. Hacker sehen dort nicht nur schnell und einfach alles, was geschieht, sondern können sich über die Lücke auch in weiteren vor Ort genutzten Systemen festsetzen und diese als Angriffswerkzeug missbrauchen. Nutzer VdS-anerkannter Anlagen haben solche Probleme nicht – auf genau derartige Mängel prüfen wir schließlich.“

Häufig entsteht das Problem, weil der Fernzugriff per App ermöglicht werden soll. Wichtige Hilfestellungen für eine sichere Umsetzung finden Entwickler in den kostenlos erhältlichen Richtlinien VdS 3169 (einfach im Suchfeld auf vds-shop.de „3169“ eingeben).

Dr. Florian Scharr
Public Relations
Tel.: +49 (0)221 77 66-6417
Fax: +49 (0)221 77 66-311
E-Mail: FScharr@vds.de

VdS Schadenverhütung GmbH
Ein Unternehmen des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V.

Amsterdamer Str. 172–174
50735 Köln

www.vds.de

BU Hack: Selbst im Sicherheitsbereich eingesetzte Cloud-Lösungen sind oftmals viel zu leicht angreifbar. Jüngstes Beispiel: Neun Millionen wegen eines unsicheren Bauteils leicht zu hackende Videokameras – 1,3 Millionen davon in Deutschland im Einsatz.

Pressekontakt:

Dr. Florian Scharr
Public Relations
Tel.: +49 (0)221 77 66-6417
Fax: +49 (0)221 77 66-311
E-Mail: FScharr@vds.de

Über VdS

VdS gehört zu den weltweit renommiertesten Institutionen für Unternehmenssicherheit. Rund 500 Experten bieten ein einzigartiges Dienstleistungsspektrum für Brandschutz, Security, Cyber-Security und Naturgefahrenprävention.

Das VdS-Angebot umfasst Risikoanalysen, Prüfungen und Zertifizierungen, Inspektionen von Anlagen, Auskunftssysteme zu Naturgefahren sowie ein breites Bildungsangebot. Das unabhängige Institut setzt darüber hinaus mit der Veröffentlichung von Regelwerken internationale Sicherheitsstandards.

Die optimale Absicherung unserer Partner basiert auf einem weltweit einzigartigen Schutzkonzept, dessen Zuverlässigkeit auf weit über 100 Jahren VdS-Erfahrung aufbaut und das alle Aspekte der Schadenverhütung miteinander verbindet. 30 von 30 DAX-Unternehmen sowie Entscheider auf der ganzen Welt verlassen sich auf VdS-geprüfte Wirksamkeit und Sicherheit.

Weitere Informationen unter www.vds.de

VdS Schadenverhütung GmbH
Ein Unternehmen des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V.

Amsterdamer Str. 172–174
50735 Köln

www.vds.de

Verlassen Sie sich auf Europas Nr.1 für Unternehmenssicherheit