Ronald Eikenberg

Discount-Spion

Aldi verkaufte unsicher konfigurierte IP-Kameras

Aldi hat mehrfach IP-Überwachungskameras mit denkbar schlechten Voreinstellungen verkauft. Die Geräte sind zu Hunderten fast ungeschützt über das Internet erreichbar.

Die bei Aldi verkauften IP-Überwachungskameras der Marke Maginon haben massive Sicherheitsprobleme: Unbefugte könnten über das Internet auf das Kamerabild zugreifen und sogar den Ton anzapfen. Zwei Modelle sind per Motor steuerbar, der Bildausschnitt ist frei wählbar. Zudem verraten die Geräte unter anderem die Passwörter für WLAN, E-Mail und FTP-Zugang ihres Besitzers. Hunderte dieser Kameras sind ungeschützt über das Internet erreichbar. Darüber hatte der Zusammenschluss Digitale Gesellschaft die c't informiert.

Drei Modelle betroffen

Die Kameras IPC-10 AC, IPC-100 AC und IPC-20 C hat Aldi mit einer Firmware angeboten, die den Fernzugriff auch dann erlaubt, wenn der Nutzer kein Passwort gesetzt hat. Dies ist fatal, da die Geräte bemüht sind, sich über das Internet erreichbar zu machen: Sie versuchen selbstständig, auf dem Router über UPnP eine Weiterleitung von Port 80 einzurichten.

Gelingt dies, kann man anschließend über http://<externe-IP-Adresse> weltweit auf die Kamera zugreifen. Ist kein Passwort gesetzt, kann fortan jeder einen Blick durch das Kameraauge werfen. Da die Modelle IPC-10 AC und IPC-100 AC mit einem Mikrofon ausgestattet sind, können Unbefugte sogar Gespräche belauschen. Ferner sind diese Geräte motorgesteuert schwenkbar, ein ungebetener Gast kann also den Bildausschnitt beliebig verändern. Alle drei Modelle können durch Infrarot-LEDs auch in der Dunkelheit sehen.

Doch die Kameras gefährden in dieser Standardkonfiguration nicht nur die Privatsphäre, sondern auch die Sicherheit ihrer Nutzer: Über den Fernzugriff kann man die Kamera-Konfiguration auslesen, mitsamt aller vom Nutzer gespeicherten Zugangsdaten. Darunter befindet sich etwa das Passwort für das WLAN, mit dem die Kamera verbunden ist. Und auch die Logins für externe Mail- und FTP-Server geben die Geräte preis, sofern der Nutzer die Mail-Benachrichtigung respektive den FTP-Upload konfiguriert hat.

Firmware-Update

Betroffene Modelle hatte Aldi Süd am 9. 3., 22. 6. und 12. 12. 2015 im Angebot, Aldi Nord am 22. 6. und Aldi Suisse am 18. 6. sowie am 24. 12. Bei der zu Aldi gehörenden österreichischen Discount-Kette Hofer wurde zuletzt am 24. 12. eine Kamera des Herstellers angeboten – da das Unternehmen nicht auf unsere Anfrage reagierte, können wir zu weiteren möglichen Terminen keine präzisen Angaben machen. Auch das Unternehmen supra, das die Maginon-Kameras vertreibt, reagierte nicht. Die drei Aldi-Ableger erklärten, dass „den Nutzern bereits seit einigen Monaten ein Firmware Update zur Verfügung steht, bei dem sie ein persönliches Passwort festlegen müssen. Wird das Update installiert, jedoch nicht das Kennwort geändert, kann der Nutzer selbst nicht mehr von extern auf die Kamera zugreifen und wird somit automatisch zum Einrichten dieser Sicherheitsvorkehrung aufgefordert."

Dennoch sind viele Kameras ungeschützt: Laut uns vorliegenden Testergebnissen kann man auf mehr als ein Drittel der Kameras, die über das Internet erreichbar sind, ohne Passwort zugreifen – es handelt sich um eine vierstellige Zahl. Einer der Gründe hierfür könnte sein, dass sich die Kameras nicht selbstständig um die Aktualität ihrer Firmware kümmern. Stattdessen muss der Nutzer aktiv werden und zunächst ein Programm auf dem PC installieren, das die Firmware aus dem Netz zieht und auf die Kamera überspielt. Einen Fernzugriff ohne Passwort verhindert die Firmware-Version 1.2 und aufwärts. Auch wenn diese seit „einigen Monaten" verfügbar ist, wurden Ende vergangenen Jahres anscheinend noch Geräte mit älterer Firmware verkauft.

Verhaltener Update-Hinweis

Um die Situation in den Griff zu bekommen, haben die drei Aldi-Unternehmen ihren Lieferanten gebeten, weitere Maßnahmen zu ergreifen. „So werden die Nutzer von unserem Lieferanten erneut eine Update-Information erhalten, mit der sie nochmals explizit darauf hingewiesen werden, ein persönliches Kennwort festzulegen. Beim Öffnen des Programmes bzw. der App werden die Nutzer automatisch auf dieses Update aufmerksam gemacht." Das Windows-Tool und die Apps sind allerdings nicht zwingend notwendig, um die Kamera zu nutzen. Wer nur den Browser-Zugriff nutzt, bekommt davon nichts mit. Ferner will Aldi überprüfen, ob und wie man die „Kundinnen und Kunden noch deutlicher über Sicherheitsvorkehrungen informieren" kann. Einen Sicherheitshinweis auf den Aldi-Seiten suchten wir jedoch vergeblich.

Jetzt handeln!

Wer eine betroffene IP-Kamera betreibt, sollte mithilfe des mitgelieferten Windows-Tools sicherstellen, dass die aktuelle Firmware installiert und ein individuelles Passwort gesetzt wurde. Hat man Passwörter für WLAN, Mail oder FTP in der Kamera gespeichert und kann nicht ausschließen, dass das Gerät ohne Zugriffsschutz mit dem Netz verbunden war, sollte man diese Passwörter sicherheitshalber ändern. Ist der Router über UPnP konfigurierbar, sollte man diese Funktion besser abschalten, um zu verhindern, dass Geräte und Programme unbemerkt Port-Weiterleitungen einrichten.

Allerdings ist selbst nach dem Befolgen aller Sicherheitsmaßnahmen Vorsicht geboten: Da der Fernzugriff der Kameras unverschlüsselt über HTTP erfolgt, kann sich ein Mitlauscher bei der Nutzung ebenfalls dauerhaften Zugang zur Kamera verschaffen. Man sollte die Verbindung also – wenn überhaupt – nur in vertrauenswürdigen Netzen aufbauen und öffentliche Netze wie Hotspots meiden. (rei@ct.de)

Die bei Aldi und Hofer angebotenen IP-Kameras Maginon IPC-10 AC, IPC-100 AC und IPC-20 C sind zu Hunderten ungeschützt über das Internet steuerbar.