PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Page Screenshot

Laut Experte Francesco Ongaro von IS Group ist das brandgefährlich: «Damit löst der Betreiber das schwierigste Problem für einen Hacker: den direkten Zugriff auf die Anlage via Internet.» Hat der Hacker einmal Kontakt zu einer Steuerungsanlage, findet er meistens eine Lücke, um die Kontrolle über ein Kraftwerk oder eine Wärmepumpe zu übernehmen, denn viele Industriesteuerungen sind heutzutage veraltet und schlecht bis gar nicht geschützt. Beim Sicherheitstest fand die SonntagsZeitung in Zürich zum Beispiel drei Geräte zur Überwachung von Abwasser-

Pumpstationen. Diese Stationen überbrücken Höhenunterschiede im Abwassernetzwerk der Stadt Zürich. Ohne Passwort kamen die Journalisten mit einem Internetbrowser direkt auf die Überwachungsgeräte. Eine direkte Manipulation der Wasserpumpen sei über die Geräte nicht möglich, da die Steuerungen getrennt liefen, sagt die Betreiberin, die Entsorgung und Recycling Zürich (ERZ). Doch für einen Hacker ist dieses Gerät nur der erste Schritt. Ist er erst mal im internen Netzwerk, findet er in der Regel Zugang zu den Maschinen, in diesem Fall den Pumpen.

Auf den Hinweis, dass ihre Steuerung im Internet zugänglich ist, reagierte die ERZ überrascht. Die Geräte seien erst kürzlich ersetzt und offenbar nicht richtig konfiguriert worden. «Das sollte sicher nicht so funktionieren. Wir werden den Prozess beim Aufsetzen solcher Geräte überprüfen, damit das nicht mehr vorkommt.» Das Unternehmen hat die Geräte nach dem Hinweis vom Internet getrennt und neu konfiguriert.

Weniger einsichtig zeigte sich das Waadtländer Kantonsarchiv. In Lucens, unweit von Lausanne, unterhält der Kanton ein Lager für Kunstschätze. Meterdicke Betonwände und ein ausgeklügeltes Lüftungssystem schützen Tausende wertvoller Objekte, von historischen Büchern über Gemälde bis zu Tierpräparaten. Vor vier Jahren hat der Betreiber eine Steuerungsanlage direkt ans Internet gehängt. Wie in Basel kann man das System mit einem längst bekannten Trick übernehmen.

Wer will, kann die Luftfeuchtigkeit und Temperatur im Lager nach Belieben manipulieren. Betroffen seien nur Bücher, keine wertvollen Objekte, sagt das Kantonsarchiv und liess das System nach dem Hinweis erst mal weiterlaufen. Erst nach mehrmaligem Insistieren nahm der Kanton die Anlage vom Netz.

Der Sicherheitstest hat gezeigt, dass in der Schweiz vor allem mittelgrosse Anlagen schlecht geschützt sind. Bei manchen brauche es für den Zugriff nicht einmal einen Hacker, sagt Experte Ongaro: «Auf viele Anlagen kann selbst mein Cousin zugreifen.» Es fehle oft der simpelste Sicherheitsmechanismus. Zum Beispiel sollte ein Gerät nach einer bestimmten Anzahl von Zugriffversuchen den Zugang sperren. Eine Sicherung, die Ongaro fast nie antrifft. Einige Geräte sind gar ohne Passwort erreichbar.

In der Schweiz finden sich zum Beispiel Wärmeverbunde mit einer Leistung von mehreren Hundert Kilowatt, Fotovoltaikanlagen oder Klimasteuerungen, die jeder manipulieren kann. Eine Überlastung der Fernleitung? Das

1. ZEITUNGSARTIKEL - FAHRLÄSSIG DURCHLÄSSIG

2. IN BASEL LAG DAS SCHLIESSSYSTEM DES ST.-JAKOB-PARKS WÄHREND EINES JAHRES FÜR HACKER OFFEN

Foto: Freshfocus

2742 Steueranlagen stehen für Hacker offen, darunter selbst Systeme des St. Jakob-Stadions in Basel. Erstmals zeigt ein Test, wie es um die Sicherheit der Schweizer Infrastruktur steht und wie leicht es ist, sie zu manipuliere

Von Florian Imbach und Alexandre Haederli

38 500 Menschen fasst das grösste Stadion der Schweiz, der St.-Jakob-Park in Basel. Tausende besuchen das angeschlossene Shoppingparadies mit Läden wie Manor, C & A oder Kookai. Aber niemand dürfte ahnen, dass man das Schliess- und Kontrollsystem mit einer Lücke, die seit Monaten bekannt ist, übernehmen kann. Erst nach einem Hinweis der SonntagsZeitung hat der Betreiber das System am vergangenen Mittwoch vom Internet getrennt.

Zuvor konnte jeder das «Tür-Management-System M2010» direkt über einen Internetbrowser abrufen und dank einer Passwortlücke kontrollieren. Ein Vandale, ein Einbrecher oder gar ein Attentäter hätte den Personaleingang des Shoppingcenters in der Nacht öffnen und ungehindert unter das Stadion gelangen oder in die Läden einbrechen können. Er konnte Tür- und Sicherheitsalarme deaktivieren und die Fernalarmierung ausschalten. Er konnte aber auch einstellen, wann Zugangstüren offen stehen und wann sie geschlossen sind.

Ans Licht kam das massive Sicherheitsproblem im Rahmen des ersten systematischen Sicherheitschecks von Schweizer Industrieanlagen (siehe Box Seite 14). Durchgeführt hat ihn die italienische Sicherheitsfirma IS Group. Das Ergebnis: Mindestens 2742 Schweizer Anlagen sind gefährdet. Darunter auch Kleinkraftwerke, Kläranlagen und Produktionsbetriebe. Sie sind verwundbar, weil die Betreiber die Steuerung dieser Anlagen direkt ans Internet gehängt haben. Meist aus Bequemlichkeit, um die Anlagen aus der Ferne zu warten.

Laut Experte Francesco Ongaro von IS Group ist das brandgefährlich: «Damit löst der Betreiber das schwierigste Problem für einen Hacker: den direkten Zugriff auf die Anlage via Internet.» Hat der Hacker einmal Kontakt zu einer Steuerungsanlage, findet er meistens eine Lücke, um die Kontrolle über ein Kraftwerk oder eine Wärmepumpe zu übernehmen, denn viele Industriesteuerungen sind heutzutage veraltet und schlecht bis gar nicht geschützt. Beim Sicherheitstest fand die SonntagsZeitung in Zürich zum Beispiel drei Geräte zur Überwachung von Abwasser-

Pumpstationen. Diese Stationen überbrücken Höhenunterschiede im Abwassernetzwerk der Stadt Zürich. Ohne Passwort kamen die Journalisten mit einem Internetbrowser direkt auf die Überwachungsgeräte. Eine direkte Manipulation der Wasserpumpen sei über die Geräte nicht möglich, da die Steuerungen getrennt liefen, sagt die Betreiberin, die Entsorgung und Recycling Zürich (ERZ). Doch für einen Hacker ist dieses Gerät nur der erste Schritt. Ist er erst mal im internen Netzwerk, findet er in der Regel Zugang zu den Maschinen, in diesem Fall den Pumpen.

Auf den Hinweis, dass ihre Steuerung im Internet zugänglich ist, reagierte die ERZ überrascht. Die Geräte seien erst kürzlich ersetzt und offenbar nicht richtig konfiguriert worden. «Das sollte sicher nicht so funktionieren. Wir werden den Prozess beim Aufsetzen solcher Geräte überprüfen, damit das nicht mehr vorkommt.» Das Unternehmen hat die Geräte nach dem Hinweis vom Internet getrennt und neu konfiguriert.

Weniger einsichtig zeigte sich das Waadtländer Kantonsarchiv. In Lucens, unweit von Lausanne, unterhält der Kanton ein Lager für Kunstschätze. Meterdicke Betonwände und ein ausgeklügeltes Lüftungssystem schützen Tausende wertvoller Objekte, von historischen Büchern über Gemälde bis zu Tierpräparaten. Vor vier Jahren hat der Betreiber eine Steuerungsanlage direkt ans Internet gehängt. Wie in Basel kann man das System mit einem längst bekannten Trick übernehmen.

Wer will, kann die Luftfeuchtigkeit und Temperatur im Lager nach Belieben manipulieren. Betroffen seien nur Bücher, keine wertvollen Objekte, sagt das Kantonsarchiv und liess das System nach dem Hinweis erst mal weiterlaufen. Erst nach mehrmaligem Insistieren nahm der Kanton die Anlage vom Netz.

Der Sicherheitstest hat gezeigt, dass in der Schweiz vor allem mittelgrosse Anlagen schlecht geschützt sind. Bei manchen brauche es für den Zugriff nicht einmal einen Hacker, sagt Experte Ongaro: «Auf viele Anlagen kann selbst mein Cousin zugreifen.» Es fehle oft der simpelste Sicherheitsmechanismus. Zum Beispiel sollte ein Gerät nach einer bestimmten Anzahl von Zugriffversuchen den Zugang sperren. Eine Sicherung, die Ongaro fast nie antrifft. Einige Geräte sind gar ohne Passwort erreichbar.

In der Schweiz finden sich zum Beispiel Wärmeverbunde mit einer Leistung von mehreren Hundert Kilowatt, Fotovoltaikanlagen oder Klimasteuerungen, die jeder manipulieren kann. Eine Überlastung der Fernleitung? Das Ausbrennen eines Heizkessels? Oder die Verwandlung eines Grossraumbüros in eine Tropenzone? Mit wenigen Klicks erledigt. Will jemand dem Land Schaden zufügen, hat er damit Tausende Ziele. Experte Ongaro erklärt, wie das funktioniert: «Ein Hacker entwickelt beispielsweise einen Zugriff auf die zehn am häufigsten genutzten Geräte in der Schweiz. Danach kann er Hunderte Anlagen gleichzeitig angreifen.» Eine Attacke auf mehrere kleine Energieproduzenten kann sogar eine Kettenreaktion provozieren, die zu einem grossen Stromausfall führt.

Solche koordinierten Aktionen seien in der Schweiz bisher nicht bekannt geworden, sagt der Vizedirektor der Schweizer Fachstelle Melani, Max Klaus. Doch unsichere Industriesteuerungen sind eine grosse Sorge bei den Internetexperten des Bundes. Bei gewissen Herstellern spiele die Sicherheit eine untergeordnete Rolle, sagt Klaus. Ende Oktober publizierte die