FORTSETZUNG VON SEITE 13

Fahrlässig durchlässig

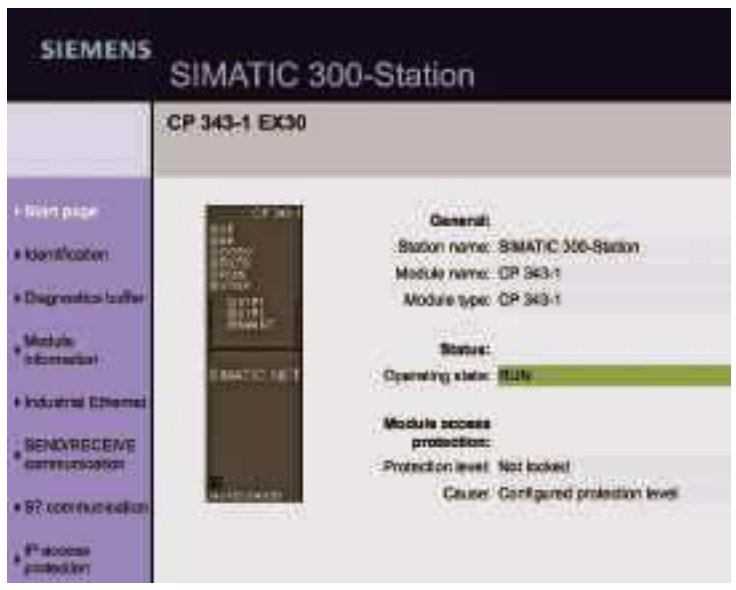
fehle oft der simpelste Sicherheitsmechanismus. Zum Beispiel sollte ein Gerät nach einer bestimmten Anzahl von Zugriffversuchen den Zugang sperren. Eine Sicherung, die Ongaro fast nie antrifft. Einige Geräte sind gar ohne Passwort erreichbar.

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 Fachstelle eine Reihe von Massnahmen zum Schutz solcher Systeme. Doch bis heute gibt es keine Mindest-Sicherheitsstandards, die Hersteller oder Betreiber einhalten müssen. Experten wie der ETH-Professor Adrian Perrig schlagen deshalb eine gesetzliche Regelung vor *(siehe Interview)*.

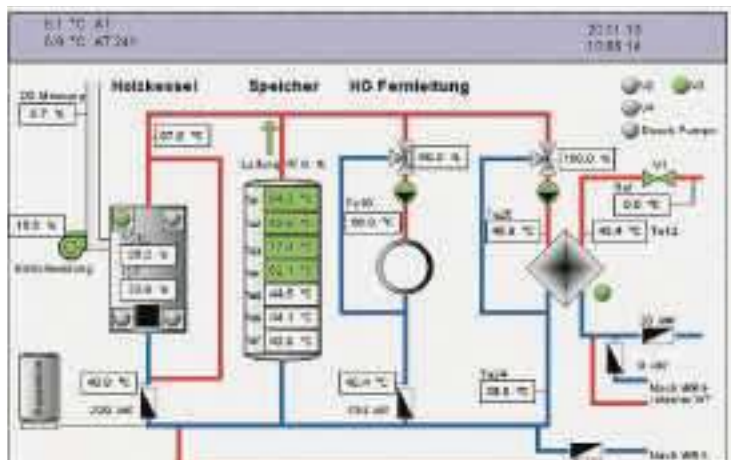
Ein Beispiel für mangelhafte Selbstkontrolle ist der Steuerungshersteller Saia-Burgess. Im Mai berichtete das Fachmagazin «c't» ausführlich über eine Sicherheitslücke bei Industriesteuersystemen des Schweizer Herstellers. Passiert ist bis heute offenbar wenig, denn immer noch sind unsichere Systeme von Saia-Burgess am Netz. Eines ist das Schliesssystem des St.-Jakob-Parks.

Saia-Burgess sagt, ihr System sei nicht dafür gedacht, direkt mit dem Internet verbunden zu werden. Ferner habe man die Kunden über die Sicherheitslücke informiert. Diese könnten mit einer Software-Aktualisierung das Passwortproblem beheben. Das hat man in Basel offenbar nicht gemerkt. Wer hier die Verantwortung für die Sicherheitslücke trägt, ist unklar. Der Stadionmanager Basel United verweist auf die Betreiberin ISS. Diese verweist auf die Eigentümerin Wincasa und der Installateur der Anlage auf den Kunden. Die Fragen der SonntagsZeitung beantwortete Wincasa nicht. Sie sagt: «Die Sicherheit ist uns sehr wichtig, so hat dieses Thema höchste Priorität.» Zum Sicherheitssystem selber und zu den einzelnen Massnahmen möchte sie «aus sicher verständlichen Gründen keine Auskunft geben». Wincasa habe das Problem erkannt und kläre, was für Massnahmen vorgenommen werden müssten.



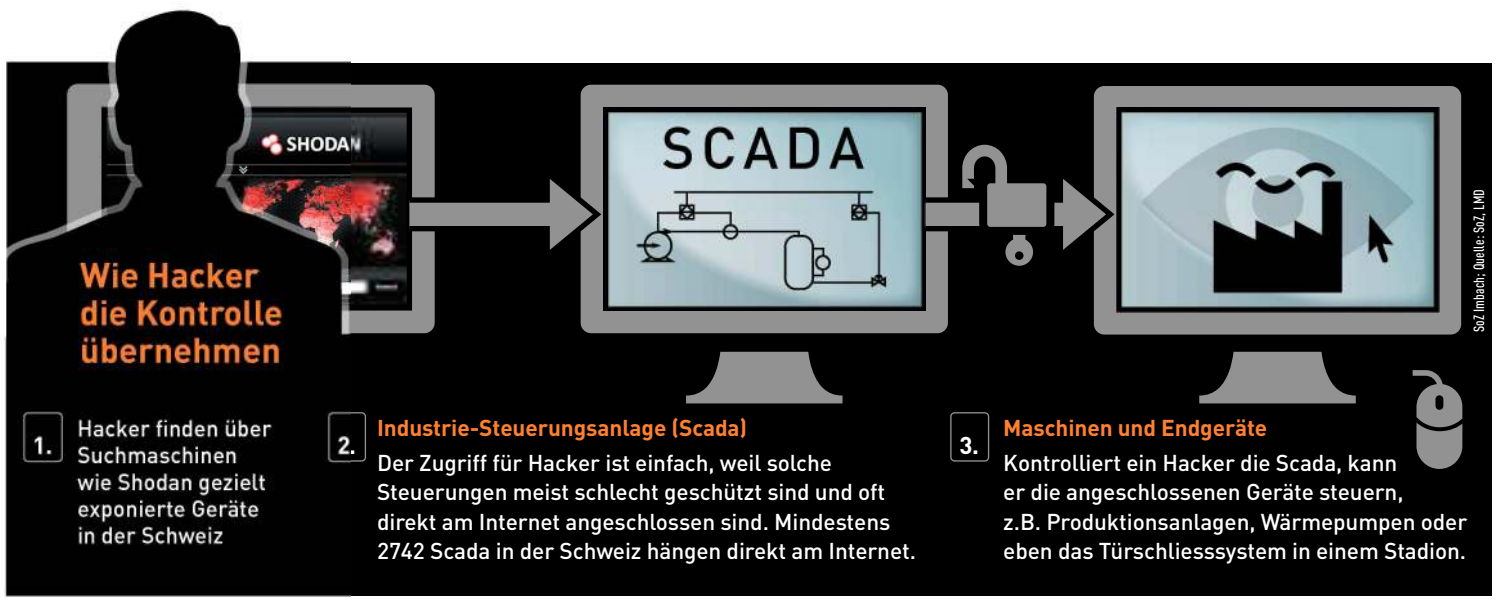
In Zürich gelang der direkte Zugriff auf drei Überwachungsgeräte von Kanalisationspumpen
FOTO: KEYSTONE

In Basel lag das Schliesssystem des St.-Jakob-Parks während eines Jahres für Hacker offen
FOTO: FRESHFOCUS



Dutzende Steuerungsanlagen wie diese waren im Netz offen zugänglich

Eine Feuchtigkeitssteuerung des «Dépôt et Abri des Biens Culturels à Lucens» (DABC)



Neugierige können ohne Passwort mithören

In einem ersten Gespräch vor Ort bestätigte die Betreiberin, dass es sich um das «Schliesssystem» handelt und damit die äusseren Zugangstüren gesteuert werden können, mit Zugang zum Einkaufszentrum, zum Stadion und Hochhaus. Eine Darstellung, die sich mit den Recherchen der SonntagsZeitung deckt. Zwei Tage später stellte sich Wincasa auf den Standpunkt, es handle sich um «kein gesamtheitliches Schliesssystem». Es gehe «ausschliesslich um eine Türe in der Aussenhülle des Shoppingcenters». Selbst wenn diese Aussage zutrifft, könnte ein Angreifer mit einem Klick das geschlossene Gebäude betreten.

ETH-Forscherin Myriam Dunn Cavelty sieht den Fall als «schwerwiegenden Sicherheitsverstoss». Dunn Cavelty beschäftigt sich seit Jahren mit Internetsicherheit und Cyberkriminalität. Die unklare Verantwortung sei typisch in solchen Fällen. «Es gibt keine klare Zuständigkeit. Man spielt sich gegenseitig den Ball zu, niemand will verantwortlich sein.»

Der Sicherheitstest zeigt, dass verantwortungsloser Umgang mit der IT in vielen Bereichen der Wirtschaft vorkommt. Eine Beratungsfirma aus Zürich etwa nutzt einen komplett ungeschützten Netzwerkspeicher, der jedem Internetnutzer offensteht. Dort finden sich Protokolle der Verwaltungsratssitzungen, detaillierte Lohnabrechnungen, Buchhaltung und Passwörter aller Mitarbeiter. Würde diese Lücke ausgenutzt, wäre die Firma innert Tagen ruiniert.

Eine renommierte Schweizer Luxusgüterfirma telefonierte, ohne es zu merken, während Monaten mit einem ungeschützten Telefonkonferenzsystem. Konkurrenten oder sonstige Neugierige können per Mausklick ohne Passwort mithören. In einem Fall stiessen die Journalisten auf einen Drucker der internationalen Fernmeldeunion in Genf, eine UNO-Organisation notabene. «Herzlich willkommen» stand da auf der Seite, die jedem Besucher offenbarte, wer gerade welche Dokumente druckte.

recherchedesk@sonntagszeitung.ch

«Die zuständigen Firmen und Hersteller müssen jetzt reagieren und ihre Systeme sichern»

Wie gut geschützt sind Steuerungsgeräte?
Solche Geräte sind die Achillesferse vieler Systeme. Wenn ein Steuergerät ein Passwort im Klartext schickt, ist das schlimm, weil ein Angreifer das einfach abhören kann. Ebenfalls schlimm sind Geräte, die nur mit einem Standardpasswort geschützt sind, was auch relativ häufig vorkommt. Besser geschützte Systeme verlangen starke Passwörter oder benützen einen zweiten Faktor, wie zum Beispiel einen Handy-Code.
Wie gut ist die Schweizer Infrastruktur geschützt?
Die Zahlen und ihre Beispiele zeigen, dass kritische Infrastrukturen vom Internet aus zugänglich sind. Über solche Geräte kann jeder von überall auf der Welt auf Anlagen zugreifen. Das ist problematisch. Die Gefahr eines Hackerangriffs ist real. Grosse Anlagen sind aber offenbar gut geschützt. Es wäre schlimm, wenn ein grosses Stromkraftwerk, etwa ein AKW, oder ein SBB-Stromverteilzentrum so exponiert wäre.

Adrian Perrig ist ETH-Professor am Institut für Informationssicherheit

Mehr als 2700 Schweizer Industrieanlagen sind verwundbar. Was muss passieren?
Solche Zahlen sollten aufwecken. Bisher ist relativ wenig passiert. Die zuständigen Firmen und Hersteller müssen jetzt reagieren und ihre Systeme sichern. Bei den Routern mit drahtlosem Internet brauchte es auch erst den Druck der Käufer, bis die Hersteller ihre Produkte stärker sicherten. Offenbar läuft es bei den Industriesteuerungen auch so.
Wie könnte man die Hersteller in die Pflicht nehmen?
Zum Beispiel mit einem Gesetz, das Betreiber verpflichtet, ihre Steuerungen zu schützen. Das zeigt Wirkung. In Kalifornien sind Firmen gesetzlich verpflichtet, beim Verlust eines Firmenlaptops alle verlorenen Daten als öffentlich verfügbar zu betrachten, mit allen rechtlichen Konsequenzen. Ausser, man schützt die Daten. Dank dieses Gesetzes sind nun praktisch alle Laptops in Kalifornien verschlüsselt. F. IMBACH

Wie zwei Italiener den Schweizern die Augen öffnen

Francesco Ongaro und Gianluca Pericoli, zwei italienische IT-Sicherheitsexperten, nahmen für die SonntagsZeitung die Schweizer Infrastruktur unter die Lupe. Ihre systematische Analyse zeigt zum ersten Mal, wie viele Industriesteuerungsanlagen (Fachwort ICS oder Scada) in der Schweiz im Internet exponiert sind. Man spricht von Industriesteuerungsanlagen, da solche Geräte in den meisten Fällen in der Industrie eingesetzt werden. Wie die Beispiele zeigen, kommen sie aber auch vermehrt in anderen Bereichen zum Einsatz.

Die Italiener listen systematisch Hersteller und Geräte auf, die per Internet erreichbar sind – ein klares Sicherheitsrisiko. Die Ergebnisse haben die Experten heute im Internet veröffentlicht. Ongaro sagt, er wolle mit der Untersuchung den Schweizern die Augen öffnen. «Die Schweiz, für ihre Genauigkeit bekannt, kümmert sich weniger um ihre Industrieanlagen als beispielsweise Italien. Im Verhältnis zur Gesamtzahl der Geräte sind in der Schweiz mehr Industrieanlagen verwundbar als bei uns.»
www.scadaexposure.com