Ausgespäht überwacht:

Industrie 4.0. Sicherheit 0.1

autor

Prof. Dr. Hartmut Pohl ist Geschäftsführender Gesellschafter der softScheck GmbH in Köln bzw. Sankt Augustin. Er ist Sprecher des Präsidiumsarbeitskreises „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik e.V. (GI)

Das Internet sowie die gesamte Telefonkommunikation im Festnetz, Mobil- und Satellitenfunk, überhaupt jede elektronische Kommunikation und die auf Servern, Clients und Stand-Alone-Systemen gespeicherten Daten werden weltweit vollständig aus- und mitgelesen – und auch manipuliert.
So werden bis zum Jahresende 2013 (heimlich) Backdoors in den 85.000 weltweit wichtigsten „strategischen Servern" installiert, um die angeschlossenen internen Netze von Unternehmen (und Behörden) nachhaltig überwachen und Daten manipulieren zu können. Dies sind die zentralen Server, Switches und Router der weltweit wichtigsten Unternehmen in der Automobil- und Energiebranche, von (Kern-)Kraftwerken, Strom- und Gasversorgung, Nahrungsmittelindustrie, Finanz- und Versicherungskonzernen, Telekommunikationsunternehmen (Internet-Infrastruktur, Mails), Medien, Unternehmen der Branchen Transport und Verkehr, Gesundheit, Wasserversorgung, Chemie- und Pharmaproduktionen oder SWIFT. Nach Ausfall einer dieser „kritischen Infrastrukturen", etwa einem weiträumigen Stromausfall, dürfte binnen fünf Tagen die Gefahr eines Bürgerkriegs drohen, weil Läden geschlossen bleiben, Tankstellen, Supermärkte sowie Kassen und die Geld- und Wasserversorgung ausfallen. Für Leib und Leben der Bundesbürger, Europäer und der Menschen in fast allen Industriestaaten besteht also akute Gefahr!

Sicherheitsprodukte: Sicherheitsprodukte generieren zwar Sicherheit, besitzen aber selbst meist nur ein sehr niedriges Sicherheitsniveau; weit überwiegend ist das Sicherheitsniveau gar nicht überprüft worden: So filtern Firewalls den Datenverkehr – der Programmcode enthält aber erfahrungsgemäß eine ganze Reihe von Sicherheitslücken. Firewalls lassen sich daher (leicht) manipulieren. Dies gilt gleichermaßen für andere Sicherheitssoftware wie Verschlüsselung, Intrusion Detection und Protection. Und es gilt grundsätzlich für Software wie Apps, Clouds, Social Media und auch für Hardware wie Herzschrittmacher, Röntgen-/Bestrahlungsgeräte und insgesamt für das digitalisierte Gesundheitswesen (Krankendaten). In die Server von Printmedien und Rundfunk bzw. Fernsehen wird eingedrungen: Auslesen geplanter Beiträge, Manipulation von Dokumenten, Adressdaten von Informanten. In Industriesteuerungen wird eingedrungen: Es werden Prozesse ausspioniert und manipuliert: Industrie 4.0? Sicherheit 0.1!

Unerkannte Gefahr: Derartige Angriffe können praktisch nicht erkannt werden. Verschlüsselung wird geknackt (z.B. Skype), Zufallszahlengeneratoren generieren Daten nicht zufällig genug oder der fragliche Rechner ist bereits kompromittiert. Diese Angriffe erfolgen nicht breit gestreut wie bei Viren, sondern sind vielmehr gezielt gegen ausgewählte Unternehmen und Behörden gerichtet. Eine der ersten dieser Targeted Attacks stellt der 2006 entwickelte Wurm „stuxnet" dar mit inzwischen mehr als zehn Nachfolgern. Diese Angriffstechniken werden – genauso wie die Backdoors – insbesondere von der organisierten Kriminalität sowie von Wirtschaftsspionage treibenden Unternehmen genutzt. Schadenssumme 2012: mehr als 4,2 Milliarden Euro. Das sind deutsche Arbeitsplätze und entgangener Gewinn von Unternehmen mit einem hohen Steueranteil.

Personenbezogene Daten: Große, personenbezogene Datenmengen erlauben es, jede Person zu klassifizieren, Dossiers zu erstellen, ihr Verhalten vorauszuberechnen und auf Basis spieltheoretischer Modelle sogar zu manipulieren. Wenn Sie dies alles nicht stört, können Sie Ihre Daten auch gleich in Social Networks speichern. Nationale Aktivitäten wie die von Nicht-Technikern geforderte „deutsche Cloud" oder ein „deutsches Internet" können gar nicht sicher sein, weil Wirtschaftskriminelle über Verbindungsrouter vom „internationalen" Internet in nationale Clouds oder Mailserver eindringen können.

Keine Hilfe: Die Politik, das EU-Parlament, weiß dies alles seit dem letzten Jahrhundert. Offensichtlich existieren mit den Verbündeten Verträge aus den Nachkriegsjahren, die eine Überwachung erlauben. Vom „No-Spy-Abkommen" ist keine Rede mehr. Die politische Frage ist allein, hat ein Präsident, hat ein Minister, eine Behörde, das gesetzliche Recht zur Überwachung und Sabotage und wo ist die demokratische, parlamentarische Kontrolle? Nehmen Sie ihre IT-Sicherheit lieber gleich selbst in die Hand; die Politik kann und wird Ihnen technisch nicht helfen. Angriffe benötigen unverzichtbar eine Sicherheitslücke, die sie ausnutzen können! BSI-Grundschutz, ISO 2700x und – bei wertvollen Daten – Stand-Alone-Systeme sind nur absolute Mindestmaßnahmen. Stand der Technik ist vielmehr ein methodischer, systematischer Security-Test der wichtigsten Anwendungen (insbesondere Threat Modeling und Fuzzing), weil nur Sicherheitslücken-freie Software allen Angriffen standhält. Wenn Sie sich so nicht absichern wollen, können Sie Ihre wertvollsten Daten auch gleich in Suchmaschinen anbieten oder Ihren Mitbewerbern zusenden. ●