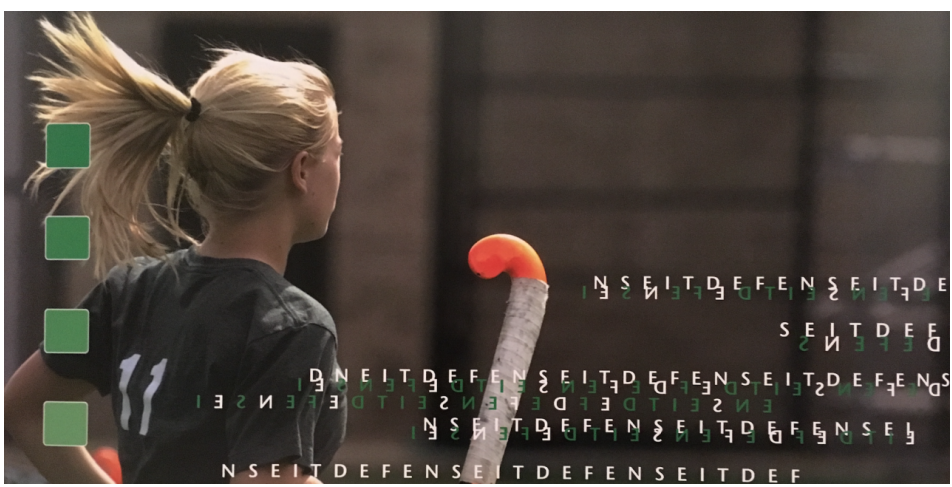
IT-Defense 2018 in München, Teil 2

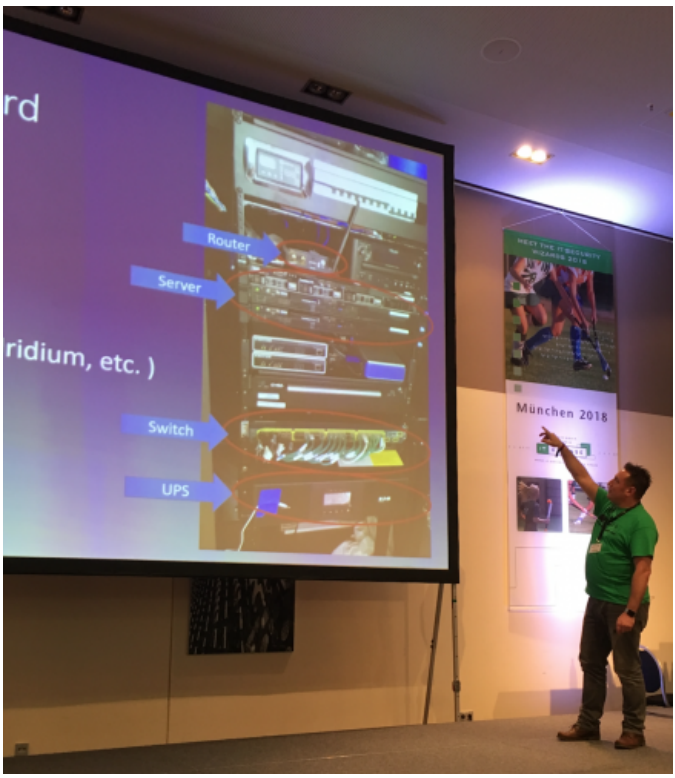
Angriffe unter der Lupe

6. Februar 2018 | Von Dr. Wilhelm Greiner.
Schlagwörter: AI, Artificial Intelligence, Biometrie, Cirosec, Hacking, IoT, IoT-Security, IT-Defense, künstliche Intelligenz, Malware, Pen-Testing, Psychometric Targeting, Social Engineering



Der Reiz von Cirosecs jährlicher IT-Sicherheitskonferenz IT-Defense liegt darin, dass sie den Bogen von High-Level-Keynotes (oder Gardinenpredigten – siehe den gestrigen LANline-Bericht) bis hin zu technisch detaillierten

Hacker-Vorträgen spannt. Die diesjährige Cirosec-Veranstaltung – mit etwas über 200 Besuchern wie immer ausgebucht – glänzte gleich mit mehreren spannenden Präsentationen.



„Die maritime IT-Security ist noch recht am Anfang“, so Yachten-Hacker Stephan Gerling. Bild: Dr. Wilhelm Greiner

So erklärte Sicherheitsexperte Stephan Gerling, wie man eine Millionen Euro teure Mega-Yacht hackt: Kommunikation wie die in der Seefahrt üblichen AIS-Signale (Automatic Identification System) zu fälschen ist laut Gerling „kein Hexenwerk“. Im Detail schilderte er einen Angriff auf den Router eine Yacht, dessen in XML geschriebene Konfigurationsänderungen per FTP und somit unverschlüsselt übertragen wurden. User-Name und Passwort waren zudem – man errät es schon – hart codiert hinterlegt. Auf Gerlings Analyse hin wechselte der Hersteller von FTP zu SSH – behielt die hart codierte Authentifizierung aber bei. Gerlings Urteil: „Die maritime IT-Security ist noch recht am Anfang.“

Der Hacker Starbug blickte auf 15 Jahre Überwindungsversuche von Biometrielösungen zurück, von der ersten Maus mit Fingerabdruckscanner über die aktuelle Gesichtsbiometrie mit 3D-Scanner und Infrarotlicht bsi zur Handvenenerkennung. Für „normale User“, so Starbug, könne man Biometrie inzwischen verwenden, für Hochsicherheitsbereiche empfiehlt er sie nach wie vor nicht. Changhoon Yoon von der KAIST Universität in Korea warnte, dass SDN (Software-Defined Networking) aus Security-Sicht noch lange nicht unternehmenstauglich ist, während Colin O’Flynn zeigte, wie leicht sich smarte Glühbirnen aus dem Hause Philipps kompromittieren lassen. Das Risiko: Die Kompromittierung kann sich Peer-to-Peer zwischen den Leuchtkörpern ausbreiten. So könnte ein Angreifer, der zehntausende ferngesteuerter Glühbirnen schnell ein- und ausschaltet, eines Tages vielleicht sogar das Stromnetz destabilisieren.

Benjamin Kollenda und Philipp Koppe von der Ruhr-Universität Bochum erläuterten Angriffe auf Prozessor-Microcode – angesichts von Meltdown und Spectre ein brandheißes Thema. Das Grundproblem sei, dass moderne CPUs Update-fähig sind – diese Updates sich aber eben kompromittieren lassen, etwa mittels des von ihnen selbst entwickelten „Angry OS“, erhältlich auf Github. Da die Software-Updates für Microkernel-Code nicht signiert sind, so die Forscher, werde jedes Update akzeptiert, sobald ein Hacker sich einmal Zugang verschafft hat. Dies ebne den Weg für Backdoors, die nur sehr schwer zu entdecken sind.

Gefahren für die Unternehmens-IT

Das Highlight unter den Technikvorträgen war

aber die Präsentation von Paula Januszkiewicz, CEO des Pen-Testing-Anbieters Cqure. Zunächst beschrieb sie, wie sie das Stereotyp der blonden, gutaussehenden Frau nutzt, um per Social Engineering in Unternehmen einzudringen (Tipp: immer zuletzt aus dem Fahrstuhl steigen, damit ein hilfsbereiter Herr die ID-kartengesicherte Tür aufhält). Anschließend diskutierte sie im Schnelldurchlauf die wichtigsten Bedrohungen der Unternehmens-IT. Problem Nummer eins, so die Expertin: „Wir haben einen jämmerlichen Umgang mit Passwörtern." Auch für diverse weitere Kernprobleme sind laut Januszkiewicz die Endanwender verantwortlich: Diese lassen ihre PCs unbeaufsichtigt und ungesichert zurück, nutzen unbekannte USB-Sticks (90 Prozent der Nutzer würden laut einer Umfrage einen fremden USB-Stick verwenden, wenn dieser das Unternehmenslogo trägt), sie fallen auf Phishing herein, vergessen Geräte in Taxis, nutzen fremde WLANs und geben ihre Passwörter an Dritte heraus.

„Wir haben einen jämmerlichen Umgang mit Passwörtern", so Security-Auditorin und Pen-Testerin Paula Januszkiewicz. Bild: Dr. Wilhelm Greiner

Doch neben menschlichen gibt es auch technische Schwächen: So demonstrierte sie, wie man, einmal ins Unternehmensnetz eingedrungen, dank Kenntnis der Windows-Schwachstellen und passender Hacking-Tools mittels Privileg-Eskalation an die Admin-Passwörter gelangt. Laut Januszkiewicz' Angaben hat ihr Unternehmen inzwischen über 200 solcher Hacking-Tool entwickelt und auf dem hauseigenen Blog bereitgestellt. Für das Auslesen des Admin-Passworts zum Beispiel nutze Cqure eine hauseigene Version des bekannten Hacking-Toolkits Mimikatz, die von Antivirenlösungen nicht erkannt werde.

Die Pen-Testerin riet dazu, neben Präventionsmaßnahmen wie laufender Schwachstellenermittlung und kontextbezogener Analyse auch den menschlichen Faktor zu berücksichtigen. Denn für das IT-Security-Fachpersonal seien Risiken eine Frage der Mathematik, für Endanwender aber eine Frage des Gefühls.

Mensch trifft künstliche Intelligenz

Diesem „menschlichen Faktor" widmete Vesselin Popov vom Psychometrics Centre der University of Cambridge einen nicht-technischen, aber ebenso spannenden Vortrag: Psychometrisches Targeting– also auf das individuelle, per AI (Artificial Intelligence) ermittelte Profil eines Anwenders ausgerichtete Information – ist, so führte der Cambridge-Mitarbeiter aus, nachweislich dazu geeignet, Entscheidungen und Aktionen der Anwender zu beeinflussen. Brisant ist dieses Thema angesichts des Umstands, dass man derzeit in den USA wie auch in Großbritannien diskutiert, in welchem Maß die Entscheidungen für Trump beziehungsweise pro

EU-Austritt mittels Social-Media-Targeting beeinflusst wurden.

Auf Facebook, so der Cambridge-Mann, könne man heute allein mittels Auswertung der Likes wesentliche Charaktereigenschaften oder auch die sexuelle Orientierung eines Nutzers eruieren. Mittels AI sei es längst möglich, die „Big Five"-Faktoren der menschlichen Psyche – Offenheit für Erfahrungen, Gewissenhaftigkeit, Extraversion (Geselligkeit), Verträglichkeit und Neurotizismus – ebenso zu ermitteln wie die Intelligenz, Lebenszufriedenheit, politische und religiöse Ansichten oder die finanzielle Risikoeinstufung eines Nutzers. AI liege dabei inzwischen sogar öfter richtig als das direkte Umfeld des Betroffenen, so der britische Forscher.

Vor diesem Hintergrund will das Psychometrics Centre Human- und Ingenieurswissenschaften näher zusammenbringen, so Popov, um „gerechtere Entscheidungssysteme" zu schaffen. Ein verantwortungsvoller Umgang mit AI setzt laut Erkenntnissen aus Cambridge folgende Schritte voraus:

- Kontrolle: Datenverwendung nur mit Zustimmung des Anwenders,
- Transparenz: der Betroffene erfährt die Ergebnisse,
- Personalisierung: Nutzung der Daten für eine verbesserte „User Experience",
- Relevanz: Datenverwendung und Ergebnis hängen direkt zusammen (also keine unerwünschte Zweitverwendung der Daten), sowie
- Dialog mit dem Anwender, um das Verfahren zu verbessern.

Angesichts des Umstands, dass AI ebenso wenig wieder verschwinden wird wie Targeted Marketing oder politische Instrumentalisierung, sei diese Forschung heute höchst relevant, so Popov gegenüber LANline. Nötig sei eine Grassroots-Bewegung für mehr Privatsphäre und sinnvolle Nutzung der IoT-Daten. Denn Targeting ermöglicht es laut Popov nicht bloß, Marketing-Maßnahmen noch effektiver zu machen, sondern kann zum Beispiel auch helfen, Risiken durch ein optimiertes Zusammenspiel von Mensch und Maschine zu mindern. So habe die Forschung gezeigt: Die Zahl der Autounfälle sinkt, wenn die Stimme des Navigationssystems auf den Charakter des Fahrers abgestimmt ist.

Die diesjährige IT-Defense punktete durch provokant vorgetragene Thesen ebenso wie durch eine Fülle von Fakten und Erkenntnissen zum Status quo in Sachen IT-Security. Die nächste IT-Defense findet von 6. bis 8. Februar 2019 in Stuttgart statt. Weitere Informationen finden sich unter www.cirosec.de und www.it-defense.de.

Dr. Wilhelm Greiner ist freier Mitarbeiter der LANline.