

Täuschungen besser erkennen

Cirosec IT-Defense, Leipzig

Täuschungen besser erkennen

geschrieben von LANline/Dr. Wilhelm Greiner am 05.02.2015

In Leipzig konnte Stefan Strobel, Geschäftsführer von Cirosec, rund 250 Teilnehmer zur dreizehnten - und wie gewohnt ausgebuchten - IT-Defense begrüßen. Highlights der diesjährigen Veranstaltung: Vorträge von Prof. Ross Anderson zur Psychologie der Sicherheit, Security-Veteran Bill Cheswick zum Wettlauf zwischen Angreifern und Verteidigern sowie Fachbuchautor und Co3-CTO Bruce Schneier zum Thema Reaktion auf Sicherheitsvorfälle (Incident Response).

Ross Anderson stellte die Frage: „Wie kann die Psychologie dem Security-Ingenieur helfen?“ Denn nach wie vor verursachen oder erleichtern Benutzerfehler Angriffe auf IT-Infrastrukturen, so Anderson. „Für die meisten Leute ist Sicherheit etwas, das sich ihrem eigentlichen Vorhaben in den Weg stellt“, so Anderson. Hinzu komme: Je mehr man über eine Aufgabe nachdenken muss, desto höher ist die Wahrscheinlichkeit eines Fehlers. Solche Erkenntnisse wurden in anderen Branchen - etwa in der Automobilindustrie oder beim Cockpit-Design im Flugzeugbau - bereits berücksichtigt.

In Krankenhäusern hingegen hat das Personal immer noch mit einer Fülle verschiedener Computer und Interfaces zu tun, und in der IT kämpfen die Anwender nach wie vor mit den Tücken der E-Mail-Verschlüsselung. Deshalb, so fordert Anderson, müsse man die richtige Art zu arbeiten zur einfachsten machen - und dies vor dem Hintergrund, dass laut Zahlen aus UK die Kriminalität nicht abnimmt, sondern schlicht zunehmend online stattfindet.

Ständig aufpoppende Browser-Warnfenster allerdings erziehen die Benutzer praktisch dazu, Warnungen zu ignorieren. Laut einem Experiment von Google hilft dabei auch das Einblenden menschlicher Gesichter nicht. Konkrete statt vage Warnungen hingegen zeigen laut Anderson durchaus einen positiven Effekt auf das Benutzerverhalten.

Schnelle und langsame Entscheidungen

Die menschliche Psyche nutzt nach aktuellen psychologischen Erkenntnissen zwei

Entscheidungssysteme: Meist, so Anderson, urteilt der Mensch spontan - und durchaus gut genug für den Alltag; manchmal aber ist ein langsames Entscheidungssystem erforderlich, also ein gründliches Durchdenken der Situation. Der Umstand, dass die spontane Entscheidung nicht immer gleich gut ist wie die durchdachte, lässt sich für Angriffe ausnutzen - durch herkömmliche Betrüger ebenso wie mittels Phishing.

Anderson berichtete von aktueller Technik zur Nachverfolgung menschlicher Bewegungen, ursprünglich entwickelt für die Filmindustrie (die CGI-Figur Gollum lässt grüßen), die sich dazu nutzen lässt, das menschliche Verhalten auf Täuschungsversuche hin zu untersuchen. Denn wie Andersons Experimente zeigten, verändert Lügen die Körperbewegungen signifikant - und dies kulturübergreifend (bei britischen ebenso wie bei asiatischen Probanden).

Täuschungsversuche ließen sich im Experiment allein anhand der Körperbewegungen zu 74,4 Prozent korrekt ermitteln, mittels Einbeziehen weiterer Parameter zu über 80 Prozent. Dieser Wert ist deutlich besser als die zirka 60 Prozent, die ein herkömmlicher Lügendetektor erzielt.

Solche Erkenntnisse könnten künftig helfen, Verbrechen effizienter aufzudecken, zum Beispiel wenn sich ein Täter im Verhör befindet. Gegen Spearphishing hingegen helfen sie leider nicht: Die Abwesenheit persönlicher Interaktion im Internet-basierten Miteinander erschwert das Aufdecken von Täuschungsabsichten. Man darf gespannt sein, was neue Techniken wie Telepresence, Motion Detection bei Spielekonsolen und mit Kameras bestückte Gadgets wie Google Glass hier in Zukunft bewirken können.