IT-Administrator vor Ort:

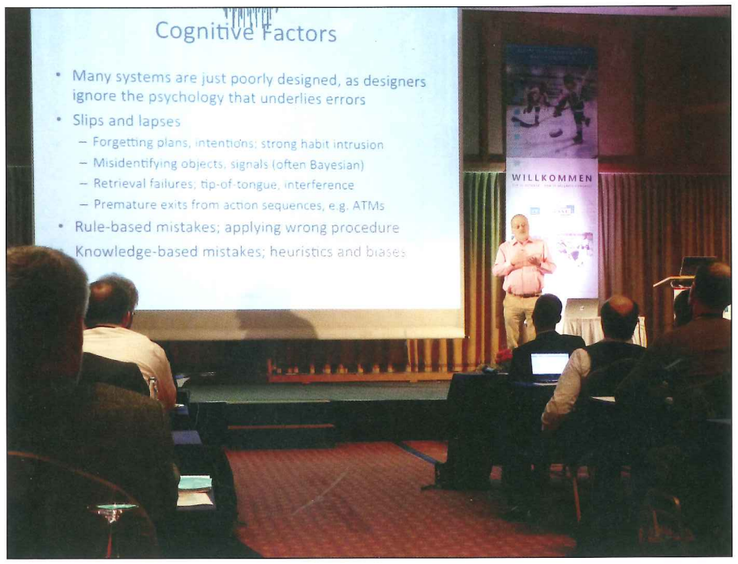
IT-Defense 2015, 4. bis 6. Februar 2015, Leipzig

Vielschichtige Sicherheit

von Daniel Richey

Zur 13. IT-Defense lud der Security-Dienstleister Cirosec nach Leipzig ein. Die rund 200 Teilnehmer erwartete ein bunter Strauß an Themen, vorgetragen von bekannten Security-Experten. Mit im Spiel: viel Psychologie.

Sie sind ein lautloser Killer in Krankenhäusern: Transfusionspumpen. Sie versorgen die Patienten mit der richtigen Menge an Medikamenten; sofern die passende Dosierung durch das Personal eingetippt wurde. Und hier liegt laut Ross Andersen, Professor für Security Engineering am Computer Laboratory der Cambridge University, ein wesentlicher Knackpunkt: Die Ziffernblöcke unterscheiden sich von Hersteller zu Hersteller. Mal angeordnet wie der Nummernblock auf einer normalen Tastatur, mal angeordnet wie Telefontasten. Damit sei schnell eine falsche Zahl eingegeben. Und dies sei nur ein Beispiel von vielen für schlechte Usability, die in Krankenhäusern oder anderen kritischen Umgebungen Leben koste.



Ross Andersen kritisierte schlecht gestaltete Benutzeroberflächen.

Hersteller sollten sich daher fragen, wie sie die Interaktion zwischen ihren Produkten und den Anwendern möglichst einfach gestalten können. Seit langem schon warnen Browser beispielsweise die Nutzer vor Gefahren, die sie jedoch meist ignorieren. Google habe mit Chrome nun herausgefunden, dass Warnungen mit einem Cartoon-Gesicht und ohne das Chrome-Logo die Berücksichtigungsrate von 30 auf 60 Prozent ansteigen ließ. Der Grund: Menschen sprechen auf Gesichter an. Überhaupt sei es deutlich effektiver, konkrete Warnhinweise auszugeben, die auch die Konsequenzen für Fehlverhalten verdeutlichen, als allgemein gehaltene.

Einfach ausgetrickst

Der Social Engineering Pentester Jayson E. Street führte dem Publikum in seinem Vortrag vor Augen, wie sich einfachste psychologische Tricks zu ausgewachsenen Sicherheitsproblemen entwickeln können. Er versucht im Auftrag von Firmen, in die zumeist gut gesicherten Gebäude oder Filialen einzudringen und an die internen Rechner zu gelangen. Einmal sollte er beispielsweise in eine Bankfiliale im Libanon vordringen, was ihm auch ohne Schwierigkeiten gelang. Dabei sei er schlicht hineingelaufen und hat sich in den geschlossenen Bereich gemogelt.

Ihm diente dabei der Social Engineering-Trick, die Mitarbeiter zu überzeugen, dass er Computer-Techniker sei und an die Rechner müsse. Die Mitarbeiter hätten ihn irgendwann sogar direkt angesprochen und darum gebeten, bestimmte IT-Probleme zu beheben. Die Möglichkeiten, die ihm als richtiger Angreifer zur Verfügung standen, hätten gut für einen großangelegten Betrug gereicht. Dazu gehörten der Username und das Passwort einer der Mitarbeiter.

Die Grundlage für erfolgreiches Social Engineering: Menschen möchten anderen Menschen gerne glauben. Für Mitarbeiter sei es daher generell wichtig, für alle Eventualitäten ausgebildet zu sein. Die Bankmitarbeiter hätten wohl anders reagiert, wenn der Pentester eine Skimaske und Waffe getragen hätte. Deshalb gelte der Grundsatz, dass Fremde immer Gefahr bedeuten. Sie müssten entweder kritisch gefragt werden, was genau sie tun, oder gemeldet werden. Auch sollten unter dem Jahr immer wieder entsprechende Infoveranstaltungen stattfinden.

Sicheres IPv6

Sehr viel technischer wurde Fernando Gont von SI6 Networks in seinem Vortrag zur IPv6-Sicherheit. Da sich die IP-Adresse nicht ändert und Clients direkt mit ihrer IPv6-Adresse Server ansprechen, sind diese leicht identifizierbar. Die NAT-Übersetzung wie bisher entfällt. Über die Interface-ID in einer IPv6-Adresse, die auch die MAC-Adresse eines Rechners enthalten kann, ist ein Rechner sogar dann netzwerkübergreifend identifizierbar, wenn sich das Präfix der IP-Adresse ändert. Die Interface-ID macht einen Rechner also dauerhaft identifizierbar. Auch lässt sich dank der MAC-Adresse der Netzwerkkartentyp ausmachen und gezielt angreifen.

Zwar soll Scanning in IPv6-Netzen nicht mehr möglich sein, da es quasi unendlich lange dauern würde angesichts der großen Entropie der 128 Bit-IP-Adressen. Dieser immense Adressbereich wird laut Gont in der Praxis jedoch gar nicht genutzt. IP-Adressen folgen vielmehr Mustern, wie der Security-Experte im Internet bei der Untersuchung von IPv6-Server-Adressen herausgefunden hat. Die meisten Web- und Mailserver nutzen sogenannte Low-Byte-Adressen in der Interface-ID. Dabei wird immer nur das letzte Byte variiert und die ID ist nicht rein zufällig. Adress-Scans, die sich auf diese Muster fokussieren, sind dadurch möglich.

Ein Ansatz seien daher temporäre Adressen (RFC4941), bei denen sich die Interface-ID von Zeit zu Zeit ändert. Diese zufälligen Adressen ergänzen allerdings die Standard-Adresse nur und ersetzen diese nicht. Damit verwendet ein Rechner also zwei IP-Adressen. Verbindet sich ein Rechner nun mit einem Webserver, nutzt er die temporäre Adresse, um nicht dauerhaft identifizierbar zu sein. Für angebotene Dienste im Netz kann und sollte hingegen die IP-Adresse dauerhaft gleich bleiben.

Angreifbar seien solche Rechner aber dennoch, da sich die statische Adresse ja nicht ändert und gegebenenfalls vorhersehbar bleibe. Die Lösung hierfür seien "Stable Privacy-Adressen" (RFC7217). Deren Ziel ist es, mit einer Hash-Funktion eine Interface-ID zu generieren, die auf dem Netzwerk-Präfix und einem geheimen Schlüssel basiert. Damit ändert sich mit jedem Netzwerk die Interface-ID grundlegend, bleibt aber bei Rückkehr in ein zuvor genutztes Netzwerk dem Netzwerk gegenüber gleich. Durch diese zufällige Interface-ID ist es für Angreifer deutlich schwerer, das Netzwerk zu scannen, da die gesamte Entropie ausgenutzt wird. Für FreeBSD und Linux gibt es bereits Implementierungen.

Internationale Regeln für den Cyberspace

Security-Guru Bruce Schneier erläuterte die Entwicklungen im Fall des Sony-Hacks und dessen Konsequenzen für die IT-Welt. So gebe es in der IT-Community große Zweifel an den Beweisen für eine Schuld Nordkoreas. Es ergebe nicht viel Sinn, weshalb das Land Sony angreifen sollte. Für "normale Hacker" scheine es viel wahrscheinlicher. Auch liege es durchaus im Interesse Sonys, dass ein Staat der Angreifer sei. Hätte nämlich eine fremde Macht Sony angegriffen, sei Sony nicht regresspflichtig. Das Angriffsmuster sehe zudem ähnlich aus wie andere Vorfälle dieser Art von Hackerbanden. Denkbar sei ferner, dass es sich um nordkoreanische Hacker gehandelt hat, die jedoch nicht in offiziellem staatlichen Auftrag gearbeitet haben.

Am 22. und 23. Dezember 2014 wurde Nordkorea dann selbst von einer DoS-Attacke betroffen. Im Januar haben die USA dann zudem ihre Sanktionen gegen Nordkorea ausgeweitet als Vergeltung für den Sony-Hack, obwohl es in der IT-Security-Community nach wie vor Zweifel an der Schuld des kommunistischen Landes gebe.

Wie dem auch sei, der Fall verdeutlicht laut Schneier die Asymmetrie von Online-Angriffen. In der realen Welt sind Angreifer anhand ihrer Waffen identifizierbar. Panzer etwa lassen sich leicht erkennen und identifizieren. Diese Kriegsregeln gelten im Cyberspace nicht und Angreifer könnten sich verstecken. Das Opfer wisse über einen längeren Zeitraum so nicht, wer es angegriffen hat. Im Cyberspace nutzen laut Schneier dabei alle Akteure quasi die gleichen Waffen.

Politisch motivierte Angriffe seien Realität und hätten echte Auswirkungen. Schneier plädierte daher für Incidence Response-Möglichkeiten, auch ohne die Akteure dahinter zu kennen. Das gelte vor allem für kritische Infrastrukturen. Verhindern ließen sich derartige Angriffe schließlich nicht. Auch stehe der Cyberspace gerade erst am Anfang eines Wettrüstens. Im internationalen Bereich forderte der Security-Experte für die Online-Welt daher "Rules of Engagement", vergleichbar zur realen Welt.

Fazit

Die 13. IT-Defense beleuchtete das breite Spektrum der IT-Sicherheit aus verschiedenen Blickwinkeln. Dazu gehörte die User-Sicht ebenso wie die Sicht von Programmierern und Admins. Denn nur im Zusammenspiel lässt sich so etwas wie Sicherheit tatsächlich erreichen. IT