IT-Sicherheit braucht wachsame Endanwender

Cirosec IT-Defense, Leipzig (II)
IT-Sicherheit braucht wachsame Endanwender
geschrieben von LANline/Dr. Wilhelm Greiner am 06.02.2015

Auf der von Cirosec ausgerichteten IT-Sicherheitskonferenz IT-Defense in Leipzig berichtete Jason E. Street, Spezialist für Social Engineering (Ausnutzen menschlicher Schwächen) und Security Awareness (Sensibilisierung für Sicherheitsfragen), in seinem sehr amüsanten Vortag „Breaking in Bad“ über grundlegende, aber effektive Methoden des Eindringens in die Unternehmens-IT: Sogenannte Advanced Persistent Threats sind laut Street oft gar nicht nötig, ein selbstbewusstes Auftreten und ein USB-Stick mit Malware genügen völlig.

Wirkungsvoll ist Streets Erfahrung nach ein Auftreten als Techie, PC-Kundendienstmann, Lieferant („Wann haben Sie einen Mitarbeiter eines Lieferdienstes jemals nicht in Haus gelassen?“), Bewerber auf eine offene Stelle, Kunde - oder als jemand, der einfach nur mal so hereinspaziert. Auf diese Weise hat sich White-Hat-Angreifer Street vor Jahren in einer Bank in Beirut innerhalb von nur zwei Minuten und 22 Sekunden vollen Zugriff auf das Banknetzwerk verschafft - als „Auditor für USB-Laufwerke“. In einer anderen Filiale der Bank entwendete er einen PC einfach durch „Reingehen, Abschrauben, Rausgehen“ - ohne von einem Bankmitarbeiter angesprochen zu werden.

Jason Streets Tipp für unauffälliges Eindringen: einfach vor der verschlossenen Tür stehen und mit dem Smartphone herumspielen, bis jemand kommt und die Tür öffnet. Notfalls hält man das Smartphone ans Ohr und sagt ins Telefon: „Oh, ist schon OK, hier hat jemand den Schlüssel.“ Denn jemand mit einem Smartphone ist ja sicher wichtig und einer „von den Guten“, und der am anderen Ende der Leitung hätte ihn offenbar auch hereingelassen. Mit diesem einfachen Trick ist Street sogar schon bis in das Finanzamt eines US-Bundesstaats eingedrungen.

Über scheinbar Harmlose aufklären

Um solche Angriffe abzuwehren, sei es nötig, die Endanwender über scheinbar harmlose Eindringlinge - online, im Büro wie auch zu Hause - aufzuklären und den Mitarbeitern praktikable Verhaltensweisen aufzuzeigen: etwa unbekannte Besucher direkt anzusprechen oder aber das Sicherheitspersonal zu informieren. Oft wüssten Mitarbeiter nicht einmal, wen sie im Fall eines verdächtigen Fremden anrufen könnten.

Die IT sollte die Endanwender laut Street nicht als Teil des Problema, sondern als Teil der Lösung betrachten: „Sie sind das beste IDS, das es gibt.“ (IDS: Intrusion Detection System) Passende Schulungsmaßnahmen sollten laut Fachmann Street durchgängig stattfinden, nicht nur einmal pro Jahr. Fehler sollte ein Unternehmen den Mitarbeitern erkären und hilfreiches Verhalten belohnen. „Angestellte müssen sich wertgeschätzt fühlen, und das Management muss die Sicherheit ernst nehmen“, mahnt der Social Engineer.

Risikoquelle IPv6

Aber auch zu anderen Themenbereichen hatte die IT-Defense interessante Präsentationen zu bieten: So berichtete Fernando Gont von SI6 Networks über seine Bemühungen, Angriffe auf IPv6 vermeiden zu helfen, bevor IPv6 weit verbreitet ist - statt erst dann, wenn das Kind schon in den Brunnen gefallen ist. Zu den sicherheitsrelevanten Aspekten der IPv6-Adressierung zählt er zum Beispiel, dass die IIDs (Interface Identifiers) sich auch langfristig nicht ändern und somit eine langfristige Nachverfolgung der Netzwerkaktivität ermöglichen. Erschwerend kommt hinzu, dass die IID auch über Netzwerke hinweg konstant bleibt. Damit sind eindeutig identifizierbare Informationen zum Benutzer erschließbar. Zudem erlaubt das Adressierungsverfahren gerätespezifische Angriffsvektoren.

Das Ermitteln von IPv6-Netzwerkadressen sei entgegen anderslautender Gerüchte durchaus möglich, da der tatsächlich genutzte Adressraum eben *nicht* 2^64 Adressen umfasse. So verrate zum Beispiel ein Scan der Alexa-Top-1M-Websites, dass Low-Byte-Adressen anstelle wirklich zufälliger Adressen stark überproportional vertreten sind.

Die Verwendung temporärer IPv6-Adressen zusätzlich zu den statischen Adressen für Client-seitige Verbindungen wiederum sei aufwändig zu verwalten. Außerdem ließen sich Host-Scanning-Angriffe damit nicht abwehren.

Eine Alternative ist laut Gont die Erzeugung von IIDs gemäß RFC7217. Mit diesem Verfahren sind Adressen in jedem Subnetz stabil, aber die IID ändert sich dynamisch mit jedem Subnetzwechsel des Hosts. Der Draft vom April 2014 soll damit eine datenschutzfreundliche Alternative zur IID-Erzeugung auf der Basis der MAC-Adressen bilden. Zur Unterstützung der Administratoren gebe es ab sofort das IPv6 Toolkit von SI6 in Version 2.0.

Ron Gutierrez von GDS analysierte die Sicherheit von App-Wrapping-Lösungen, wie sie im MAM (Mobile-Application-Management) üblich sind. Diese Lösungen sind mitunter angreifbar, so Gutierrez, da sie zum Beispiel den Schlüssel auf dem Endgerät speichern. Gutierrez hat auf Github eine Security-Checkliste veröffentlicht, um App Wrapping sicherer zu gestalten.

Jeremiah Grossman, Gründer und CEO des Application-Security-Unternehmens Whitehat Security, diskutierte Schwächen auf Anwendungsebene. Das häufigste Problem ist laut Grossman inzwischen unzureichender Schutz auf dem Transport Layer, gefolgt von Informationsabfluss auf Website-Ebene und dem Klassiker XSS (Cross-Site Scripting). Der Großteil der Websites sei häufig oder gar durchgängig angreifbar, und dies gelte branchenübergreifend.

Bei einer Kundenumfrage von Whitehat Security ergab sich, dass ein Viertel der befragten Unternehmen im vergangenen Jahr einen Einbruch zu verzeichnen hatten - und dass in 56 Prozent der Unternehmen niemand für solche Einbrüche zur Rechenschaft gezogen wird. Die Durchschnittszeit für das Beheben der Lücke lag zwischen 108 und 129 Tagen - und damit immer im Bereich von Monaten.

Nur 17 Prozent der befragten Unternehmen melden entdeckte Schwachstellen täglich an ihre Entwicklungsabteilung. Grossman plädierte für eine Kontrolle der Zeit, die erforderlich ist, um Lücken zu schließen, sowie für konsequentes Einbeziehen der Security Reviews in die Qualitätssicherung der Softwareentwicklung: Gefragt sei mehr sichere Software, nicht mehr Sicherheitssoftware.