Cirosec IT-Defense, Leipzig

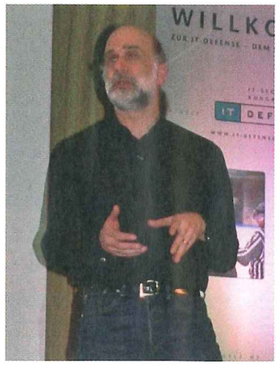
Kein „Norton Anti-Nordkorea“

Auf Cirosecs Security-Konferenz IT-Defense, die dieses Jahr zum 13. Mal stattfand, reichte das Spektrum der spannenden Vorträge von psychologischen Aspekten der Sicherheit über Social Engineering und das Hacken biometrischer Authentifizierung bis zu einem Vortrag von Firewall-Urgestein Bill Cheswick zur Lage der IT-Branche. Ein Highlight war Bruce Schneiers Diskussion des Sony-Hacks.

Der renommierte IT-Security-Vordenker Bruce Schneier ist seit Kurzem als CTO bei dem auf Incident Response spezialisierten Anbieter Co3 tätig. Doch aus aktuellem Anlass beschäftigte er sich in seinem Vortrag nicht allgemein mit der Reaktion auf Vorfälle, sondern mit dem kürzlich viel diskutierten Einbruch in das Netzwerk von Sony Pictures Entertainment, der angeblich durch oder im Auftrag von Nordkorea erfolgt sein soll. Nach dem Einbruch wurden vier bis dahin unveröffentlichte Spielfilme von Sony auf Video-Sites gepostet und eine Fülle interner Kommunikation öffentlich gemacht, sodass dem Konzern beträchtlicher wirtschaftlicher Schaden und ein signifikanter Image-Verlust entstanden – das Horrorszenario jedes IT-Sicherheitsverantwortlichen.

Laut Schneier, der die Nachrichten zum Sony-Hack genau verfolgt und ausgewertet hat, startete der Angriff im September mittels Spearphishing (gezielter Infiltration), die Angreifer seien dabei sehr umsichtig und geduldig vorgegangen. Am 24. November hätten die Hacker dann dank Zugriff auf das komplette Sony-Netzwerk begonnen, Daten in großem Umfang abzuziehen. Einige Anwender seien so schlau gewesen, ihre Rechner auszustecken, doch der Abfluss kritischer Daten sei dennoch sehr umfangreich ausgefallen.

Denn neben der unerwünschten Veröffentlichung von vier Filmen, bevor diese in die Kinos kamen, brachten mehrere Leaks internen Sony-Materials allerlei Peinliches zum Vorschein: So erfuhr man unter anderem, dass Sony seinen weiblichen Filmstars deutlich weniger zahlt als den



Bruce Schneier erläuterte auf der IT-Defense den Angriff auf Sony. Bild: Dr. Wilhelm Greiner

männlichen, und dass die Führungsriege des Konzerns in internen Nachrichten den US-Präsidenten Obama ebenso beleidigt hat wie die eigenen Schauspieler. Zudem wurden interne Nachrichten zahlreicher weiterer Sony-Mitarbeiter bekannt – für die Betroffenen ein beklemmender Bruch der Vertraulichkeit, selbst wenn nichts Dramatisches zum Vorschein kommt.

„Was den Einbruch bei Sony von den vielen alltäglichen Vorfällen abhebt“, so Bruce Schneier im LANline-Interview am Rande der IT-Defense, „ist der Umstand, dass hier nicht einfach eine Kundendatenbank entwendet wurde. Der Einbruch hat enthüllt, dass Führungskräfte von Sony sich wie Idioten verhalten haben. Und weil es in jedem Unternehmen Führungskräfte gibt, die sich wie Idioten verhalten, herrscht nun große Angst – nicht um Kundendaten, sondern um die eigenen Daten.“ Auch bei Co3 habe man deshalb steigende Nachfrage verzeichnet.

Einen neuen Trend stelle dies aber nicht dar, so Schneier zu LANline: „Solche Fälle gab es schon, man denke an die Einbrüche bei HB Gary (einer Sicherheitsfirma, der Angriff erfolgte 2011, d. Red.) oder Saudi Aramco (einem Ölkonzern, 2012, d. Red.). Solche Angriffe sind selten, aber sie kommen immer wieder vor.“ Sony habe es den Angreifern aber erstaunlich leicht gemacht. So seien zum Beispiel Passwörter in einer Plaintext-Liste mit dem Namen „Passwords“ gespeichert gewesen – ein unglaublich dummer Anfängerfehler, zumal Sony ja schon einmal Ziel eines Angriffs auf sein Playstation-Netzwerk gewesen war.

Verwirrung um Hintergründe

Einigermaßen mysteriös, so Schneier in seinem Vortrag, sind die Hintergründe des Angriffs: Die Hackergruppe Guardians of Peace bekannte sich zur Tat und verwies später als Begründung auf Nordkorea, denn eine Satire über Nordkoreas Machthaber Kim Jon-un stand damals bei Sony kurz vor dem Kinostart – diese Verbindung erstellten die Hacker aber erst, *nachdem* US-Medien über diese Option berichtet hatten. Am 19. Dezember – also gerade einmal drei Wochen nach dem Angriff – gab das FBI dann offiziell bekannt, man wisse, dass Nordkorea hinter dem Angriff steckt: Die Angreifer hätten vergessen, ihre IP-Adressen zu verschleiern.

Bei Schneier, wie bei vielen Sicherheitsexperten, löste dies Stirnrunzeln aus: „Es ergibt für Nordkorea eigentlich absolut keinen Sinn, Sony anzugreifen.“ Denn schließlich sei ein Filmstudio nicht Teil der kritischen Infrastruktur der USA wie zum Beispiel die Stromversorger und deshalb ein überraschendes Ziel für einen staatlich gelenkten IT-Angriff – Politsatire hin oder her.

Umgekehrt habe man aber auf US-Seite großes Interesse, den Angriff Nordkorea in die Schuhe zu schieben: Sony muss gemäß US-Recht mit Klagen und Schadenersatzforderungen rechnen; da ist es bequem, den Fall einer fremden Macht anlasten zu können. Für die US-Behörden mit ihrem riesigen Überwachungsapparat wiederum ist es wichtig, den Eindruck zu erwecken, man könne solche Angreifer schnell identifizieren – schon um Nachahmer abzuschrecken. Schneier gab aber zu bedenken, dass alternative Theorien wie etwa die eines Insider-Angriffs ebenfalls wenig plausibel sind.

Der Vorfall, so Schneier, zeige exemplarisch grundlegende Probleme der IT-Sicherheit im Zeitalter digitaler Kriegsführung („Cyberwar“) auf: Im herkömmlichen Krieg könnten sich nur Staaten teures Equipment wie Panzer leisten, und laut Kriegsrecht seien die Besitzer auf den Waffen kenntlich zu machen. Im digitalen Raum hingegen nutzten einzelne Hacker die gleichen Waffen wie staatliche Cyberwar-Operationen – und die Zuordnung zu einem Täter sei langwierig, wenn nicht gar überhaupt unmöglich.

Das Bedenkliche, so Schneier: „Wir alle können Ziel eines solchen Angriffs werden.“ Ziel müsse deshalb eine solide Verteidigung sein – auch gegen Angriffe, die sich nicht zuordnen lassen: „Im Cyberspace weiß man nicht, wer einen angreift und warum.“

Gefordert sind deswegen laut Bruce Schneier Konzepte und Prozesse für die effektive Reaktion auf Sicherheitsvorfälle, denn mit Sicherheitsprodukten sei das Problem nicht zu lösen: „Man wird niemals ein ‚Norton Anti-Nordkorea‘ kaufen können“ so Schneier. Auf staatlicher Ebene wiederum brauche man internationale Verträge, um den Cyberkrieg zu regeln.

Während Schneier ein düsteres Bild der Zukunft zeichnete, zeigte sich Firewall-Pionier Bill Cheswick in seinem Vortrag optimistisch: Zwar habe die IT-Sicherheit in letzter Zeit kaum Fortschritte gemacht, und nach wie vor beeinträchtigten fehlerhafter Code und mangelndes Interface-Design die IT-Sicherheit. Doch im Vergleich zur Automobilindustrie befinde sich die IT in jenen Flegeljahren, in denen es noch keine Gurtpflicht gab.

Zwei weitere Berichte zu den Präsentationen auf der IT-Defense 2015 in Leipzig finden sich auf www.lanline.de unter http://lanl.in/1LLuZaO sowie http://lanl.in/1LPUJmD.

Dr. Wilhelm Greiner

Auf LANline.de: **wgreiner**