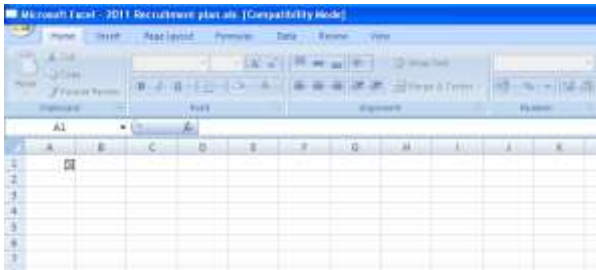


F-Secure entschlüsselt Cyberattacke auf Lockheed-Martin

Nach 5-monatiger Suche stößt Virenxperte Original-Schadcode des RSA-Exploits auf

München, 30. August 2011 – Bereits am 3. März 2011 wurde das bis dato als absolut sicher geltende asymmetrische kryptographische RSA-Verfahren – Akronym aus den ersten Buchstaben der Erfinder Ronald L. Rivest, Adi Shamir und Leonard Adleman – von Hackern mittels einer gezielten E-Mail-Attacke geknackt. Vermutlich zielte der Angriff auf die Ausspähung militärischer Geheimnisse des weltweit größten Rüstungsunternehmens Lockheed-Martin ab, das seine Daten mittels RSA verschlüsselt hatte. Jetzt stöberte der finnische Sicherheitsexperte Timo Hirvonen von F-Secure nach intensiven Nachforschungen die ursprüngliche Nachricht samt kontaminiertem Dateianhang auf.



Timo Hirvonen wies nach, dass Anfang des Jahres vier Angestellte des Unternehmens EMC, das die gesamte Infrastruktur für RSA zur Verfügung stellt, eine gefälschte E-Mail des Karriereportals Beyond.com mit dem Betreff „2011 recruitment plan“ und einem

Excel-Dateianhang erhalten hatten. Im Textteil der Mail befand sich lediglich eine Zeile: „I forward this file to you for review. Please open and view it.“. In der Excel-Datei hingegen befand sich ein Flash-Objekt, das bei einem Klick automatisch einen „Poison-Ivy-Backdoor-Trojaner“ installierte. Dieser verband sich mit good.mincesur.com, von wo aus die Hacker vollen Zugriff auf die befallenen Rechner erhielten. Zum Zeitpunkt des Geschehens handelte es sich bei dieser Excel Schwachstelle um einen noch unbekanntem Zero Day Exploit. Über die befallenen Rechner konnten die Hacker weiter in das Firmennetzwerk vordringen, bis Sie zu den Unterlagen gelangten, die Ihnen erlaubten, den Sicherheitsmechanismus der RSA SecurID Tokens zu knacken. Dabei handelt es sich um einen Hardware-



Schlüssel, der jede Minute ein aus sechs Ziffern bestehendes Passwort generiert, womit sich jeder Nutzer am Rechner oder im Netzwerk einloggen kann. Diese Schlüssel kamen auch bei Lockheed Martin zum Einsatz, was offenbar das eigentliche Ziel des Angriffs war. Denn im Mai berichtete Lockheed Martin von einem Angriff auf das Firmennetzwerk über die SecurID Schlüssel. Wie das Unternehmen mitteilte, konnten trotz des überraschenden Angriffs keine geheimen Unterlagen entwendet werden. RSA hingegen musste in Folge weltweit alle SecurID Tokens austauschen.

Weitere Informationen erhalten Sie unter:

<http://www.f-secure.com/weblog/archives/00002226.html>

twitter.com/fsecure_de

facebook.com/f-secureDE