Mailhilfe Newsletter Nr. 176 vom 06. September 2007

Trojaner im Bundeskanzleramt und die Auswirkungen

Eine Überprüfung durch den Verfassungsschutz und das Bundesamt für Sicherheit in der Informationstechnik hat laut einem Spiegel-Bericht ergeben, dass zahlreiche Computer der Bunderregierung mit Spionageprogrammen aus China infiziert sind. Neben dem Bundeskanzleramt seien auch das Wirtschafts- und Forschungsministerium mit Hilfe von unbemerkt eingeschleusten Trojanern ausspioniert worden.

Dieser Zwischenfall macht deutlich, dass selbst Computersysteme der höchsten Sicherheitsstufe nicht ausreichend vor Hackerangriffen geschützt sind und bestätigt die Erkenntnis, dass die traditionellen Sicherheitssysteme mit der hohen Menge von täglich bis zu 3.000 neuen Bedrohungen und Angriffsmustern völlig überfordert sind und keinen zuverlässigen Schutz bieten.

Die expotentiell steigende Bedrohungsmenge macht ein Umdenken notwendig: 3.000 neue Malware-Exemplare täglich bedeuten 90.000 neue Bedrohungen pro Monat. Tendenz steigend. Durch diese stetig wachsende Anzahl wird das Volumen der traditionellen Virensigantur-Dateien immer gewaltiger, so dass die konventionellen Sicherheitslösungen bereits heute unter dieser Last extrem leiden. Des Weiteren können bei diesem Malware-Aufkommen entsprechende Signaturen kaum noch zeitnah zur Verfügung gestellt werden. Panda Security hat bereits vor Jahren auf diesen Trend mit dem innovativen Intrusion Prevention System „TruPrevent“ reagiert. TruPrevent arbeitet signaturunabhängig. Schädliche Malware wird hier über eine Verhaltensanalyse aufgespürt und beseitigt.

Panda Security setzt nun eine weitere Methode gegen die aktuelle und zukünftige Bedrohungssituation ein. Mit dieser, „Collective Intelligence“ genannten Technologie, haben Unternehmen die Möglichkeit, in Echtzeit Datenbestandteile an ein Panda-Server-Kollektiv zu übertragen. Dort finden neueste Scan-Technologien Anwendung, die auf lokalen Systemen aufgrund der Intensität der Rechenleistung nicht angewendet werden können.

Panda Security’s „Collective Intelligence“ findet bereits Anwendung im Online-Dienst „MalwareRadar“ (www.malwareradar.com). Dieser Dienst gibt Unternehmen die Möglichkeit, sich eine zweite Meinung über den aktuellen Sicherheitsstatus innerhalb ihres Netzwerks einzuholen. MalwareRadar findet u. a. aktive und latente Malware, ungepatchte Systeme, potentielle Schwachstellen und Angriffspunkte, die das Einschleusen von Spionageprogrammen ermöglichen. Es ist zudem in der Lage, die identifizierte Malware unschädlich zu machen. Abschließend erhält der Nutzer ein detailliertes Reporting über das aktuelle Schutz-Niveau sowie konkrete Hinweise, wie dieser erhöht werden kann.

Im Rahmen der aktuellen Aktion des Verfassungsschutzes des Landes NRW gegen die Wirtschaftsspionage, beteiligt sich auch Panda Security an dieser Kampagne und bietet Unternehmen die Möglichkeit, Ihre Netzwerksysteme kostenfrei mit MalwareRadar-Audits auf Schwachstellen und Schädlinge zu überprüfen.

Die aktuellen Statistiken sprechen für sich und machen deutlich, dass der Spionagefall im Bundeskanzleramt kein Einzelfall ist: in 75% aller durch Panda MalwareRadar überprüften Unternehmens-Netzwerke ist Malware gefunden worden. Von allen gescannten PC’s waren lediglich 59% malwarefrei.

weitere Informationen unter: http://www.panda-software.de/malwareradar