erwartet. Bei der Untersuchung der Whistleblowing-Meldestelle des Bundes stellte der EDÖB fest, dass eine Datensammlung vorliegt, und forderte die zuständige Behörde auf, ihrer gesetzlichen Anmeldepflicht nachzukommen. Die Aufzeichnung von Telefongesprächen der Beschäftigten in den Call Centers der Schweizerischen Post, die der EDÖB aufgrund von Hinweisen einer Gewerkschaft näher abklärte, hat sich als datenschutzkonform erwiesen. Zudem wurde im Rahmen der Schengen-Zusammenarbeit das Generalkonsulat der Schweiz in Dubai kontrolliert, wobei das Augenmerk der Datenbearbeitung beim Vergabeverfahren für Schengen-Visa galt.

Weiter nahm der EDÖB zu verschiedenen Gesetzgebungsprojekten Stellung, unter anderem zur Revision des Publikationsgesetzes. Dabei wirkte er darauf hin, dass Massnahmen vorgesehen werden, um Missbräuche im Zusammenhang mit behördlichen Publikationen im Internet zu vermeiden. Im Finanzbereich äusserte er sich zur Revision des Steueramtshilfegesetzes, wobei er das Verfahren der nachträglichen Information der beschwerdeberechtigten Person bemängelte. Sein Änderungsantrag wurde vom Bundesrat jedoch abgelehnt. Erfolgreich war hingegen seine Intervention in Sachen elektronisches Patientendossier, wie der im Berichtsjahr vorgelegte Gesetzesentwurf zeigte. Mehrere Verbesserungen zugunsten der Privatsphäre der Patienten wurden darin aufgenommen, darunter namentlich der Verzicht auf die Verwendung der Sozialversicherungsnummer als Patientenidentifikator im eHealth-Bereich.

Der vollständige Tätigkeitsbericht befindet sich auf *http://www.edoeb.admin.ch/dokumentation/00153/01174/index.html?lang=de*

Palo Alto Networks: Neue Quelle für Cyber-Bedrohungen

Palo Alto Networks (*https://www.paloaltonetworks.com/*) weist am 22.07.2014 darauf hin, dass Cyber-Kriminelle in Nigeria im großen Stil weiterentwickelte Malware-Aktivitäten ausführen, die sich nun auch gegen Unternehmen richten. Diese zählten bislang nicht zu deren primären Zielen. Unter dem Titel „419 Evolution" hat Unit 42, das Threat Intelligence Team von Palo Alto Networks, heute einen neuen Bericht zu diesem Thema veröffentlicht. Darin wird dargestellt, wie die Kriminellen jetzt auf die gleichen Werkzeuge zurückgreifen, die hochversierte Hacker und Spione einsetzen, um unternehmenskritische Daten aus Unternehmen zu stehlen.

Nigerianische Kriminelle sind berüchtigt für die Ausführung von „419"-Phishing-Betrügereien, benannt nach dem relevanten Paragrafen 419 des nigerianischen Strafgesetzbuchs. Dabei wird versucht, an Kreditkartendaten oder persönliche Daten von Personen zu gelangen. Im Laufe der letzten Jahre haben sie jedoch ihre Fähigkeiten erweitert, um Mithilfe von fortschrittlicheren Methoden auch Unternehmen ins Visier zu nehmen. Die Forscher von Palo Alto Networks identifizierten diese Aktivitäten und Techniken, benannt mit dem Codenamen Silver Spaniel, mithilfe von WildFire, ein System, das in der Lage ist, Cyber-Bedrohungen in einer virtuellen Sandbox-Umgebung schnell zu analysieren.

Die wichtigsten Forschungsergebnisse:

- Neben anderen Methoden verwenden die Kriminellen auch Remote-Administration-Tools (RATs), die über Untergrundforen zur Verfügung stehen, einschließlich der kommerziellen RATs wie NetWire, die eine vollständige Kontrolle über die infizierten Systeme ermöglichen.
- Angriffe, die Parallelen zu Silber Spaniel aufweisen, kamen bislang aus Osteuropa oder wurden von feindlichen Spionagegruppen ausgeführt; Unternehmen haben gewöhnlich nicht dedizierte Ressourcen, um diese potenziell sehr effektiven Spammer aus Nigeria abzuwehren.
- Herkömmliche Antivirus-Programme und Legacy-Firewalls sind unwirksam, weil Silver-Spaniel-Angriffe speziell dafür konzipiert sind, genau diese Technologien zu umgehen.

„Die Silver-Spaniel-Malware-Aktivitäten haben ihren Ursprung in Nigeria und es kommen stets ähnliche Taktiken, Techniken und Verfahren zum Einsatz. Die Akteure zeigen zwar nicht ein so hohes Maß an technischem Scharfsinn, stellen aber dennoch eine wachsende Bedrohung für Unternehmen dar, die bisher nicht zu ihren primären Zielen zählten."

Als Schutzmaßnahme gegen die NetWire RAT hat Palo Alto Networks ein kostenloses Tool veröffentlicht, um Befehls- und Steuerungsdatenverkehr zu entschlüsseln und zu decodieren sowie Daten aufzuspüren, die von Silver-Spaniel-Angreifern gestohlen wurden. Dieses ist verfügbar unter *https://github.com/pan-unit42/public_tools*.

Bündnis gegen Cyber-Bedrohungen wird erweitert

Die Bundesregierung und die Betreiber Kritischer Infrastrukturen haben ihre bereits seit 2007 bestehende Kooperation erneuert und Handlungsschwerpunkte für die nächsten Jahre festgelegt. In dem hierzu heute veröffentlichten Dokument „UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen" wird die weitere Zusammenarbeit zwischen Staat und Wirtschaft beim Schutz Kritischer Infrastrukturen beschrieben.

Bundesinnenminister Dr. Thomas de Maizière: „Mit den Betreibern Kritischer Infrastrukturen pflegen wir auf Grund ihrer Bedeutung für unsere Gesellschaft schon seit vielen Jahren eine besonders enge Kooperation. In Anbetracht der Allgegenwärtigkeit der Informationstechnik und der sich zuspitzenden Bedrohungslage im Cyberraum haben wir unsere Handlungsschwerpunkte überarbeitet und wollen in Zukunft noch enger zusammenrücken. Deutschland soll auch in Zukunft Vorreiter bei verlässlichen und robusten Infrastrukturen in Europa bleiben."

Die Partnerschaft UP KRITIS leistet seit ihrem offiziellen Start im Jahr 2007 einen wesentlichen Beitrag zur verlässlichen Bereitstellung der kritischen Dienstleistungen für die Menschen in Deutschland. Der Schwerpunkt liegt dabei auf einem effektiven Zusammenwirken von IT-Sicherheit und der Aufrechterhaltung kritischer Geschäftsprozesse. Leitbild des UP KRITIS ist die Zusammenarbeit zwischen Betreibern Kritischer Infrastrukturen und staatlichen Stellen zur Stärkung der Kompetenz der deutschen Wirtschaft und der Bundesregierung in gemeinsamer Verantwortung insbesondere für die IT-Sicherheit in den Prozessen Kritischer Infrastrukturen. Die Strukturen des UP KRITIS ermöglichen darüber hinaus eine Verzahnung mit den aktuellen Arbeiten an einem IT-Sicherheitsgesetz, das Mindeststandards und Meldepflichten im Bereich der IT-Sicherheit Kritischer Infrastrukturen vorsehen wird.

Das Dokument zum UP KRITIS kann von der Homepage des BMI (*http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschue-*