Schwachstellenscan als Service und lokal

Aus einem Seminar an der TU München, das Sicherheitstests von Onlinebanking-Anwendungen zum Thema hatte, entstand 2017 das Start-up-Unternehmen Crashtest Security. Die Gründer entwickelten die gleichnamige Security-Suite für automatisierte Blackbox-Pentests. Zum Teil wird mit Open-Source-Produkten gescannt, für etliche Tests haben die Firmengründer jedoch eigene Werkzeuge geschrieben. Gescannt werden Webanwendungen und API-Schnittstellen. Die bisher als Software as a Service verfügbaren Sicherheitsscans sind nun auch mit lokaler Datenhaltung möglich. Der Scanner lässt sich in Entwicklungsprozesse integrieren (DevSecOps) und soll so Sicherheitslücken früh entdecken. Es existieren verschiedene Abomodelle (Monat, Jahr), Interessenten können eine 30-Tage-Testversion erhalten. (ur@ix.de)

Severity	Finding	Noticed	Fixed
medium	**SSL Insecure Algorithm:** Signature Algorithm: MD5	☐	☐
medium	**SSL Cipher Order:** Cipherlist_128Bit is offered by the server.	☐	☐
medium	**SSL Cipher Order:** Server does not set a cipher order.	☐	☐
low	**SSL Cipher Block Chaining SSL3:** BEAST SSL3: The BEAST attack leverages weakness in the cipher block chaining (CBC) which allows man in the middle attacks.	☐	☐
medium	**SSL Cipher Block Chaining TLS1:** BEAST TLS1 The BEAST attack leverages weakness in the cipher block chaining (CBC) which allows man in the middle attacks.	☐	☐
medium	**Missing HSTS:** HSTS is not offered by the server.	☐	☐
medium	**SSL RC4:** VULNERABLE, Detected ciphers: ECDHE-RSA-RC4-SHA RC4-SHA RC4-MD5	☐	☐
high	**SSL Trust:** Certificate does not match supplied URI (same w/o SNI)	☐	☐

So sieht der Scan-Report aus, hier am Beispiel SSL (Ausschnitt).

BSI-Lagebericht: Angriffsfläche vergrößert

Bundesinnenminister Horst Seehofer und BSI-Präsident Arne Schönbohm stellten den „Bericht zur Lage der IT-Sicherheit in Deutschland 2018“ vor (siehe ix.de/ix1811010). Laut diesem sind die Angriffe in den vergangenen Monaten vielschichtiger geworden. Angriffe und Sicherheitsvorfälle wie WannaCry, NotPetya, Efail oder Spectre/Meltdown zielen auf die Grundpfeiler der IT-Sicherheit. Gleichzeitig vergrößert sich mit der zunehmenden Digitalisierung und Vernetzung die Angriffsfläche. Beides zusammen hebt die Gefährdungslage auf ein neues Niveau.

Zwar sind im Berichtszeitraum 2017/2018 größere Angriffswellen mit Verschlüsselungssoftware ausgeblieben, Grund zur Entwarnung ist das jedoch nicht. Noch immer zählen sogenannte Ransomware-Angriffe zu den aktuellen Gefährdungen. Bei Schadprogrammen und Angriffswegen beobachtet die Behörde eine große Dynamik: Bekannte Schadsoftware-Familien werden verändert, weiterentwickelt und mit immer neuen Schadfunktionen ausgestattet – was auf Verteidigerseite eine erhöhte Aufmerksamkeit und Flexibilität erfordert. Bei den zielgerichteten Angriffen, den sogenannten APTs, sieht das BSI neben dem „klassischen“ Infizieren eines Systems mithilfe von Spear-Phishing-Mails zunehmend eine weitere Variante: das Installer- und Update-Hijacking. Dazu schleusen die Angreifer auf den Webseiten oder Update-Servern der Hersteller Installationsarchive mit Schadcode ein. Nutzer infizieren so durch vermeintliches Aktualisieren ungewollt ihr System, und das Schadprogramm kann weitere Module nachladen. Diesen Angriffsvektor können die Softwarehersteller durch Absichern ihrer Webseiten und konsequentes Signieren von Updates entschärfen.

Um sich mit neuen Angriffsmethoden auseinanderzusetzen und Abwehrstrategien zu entwickeln, hat das BSI in den letzten Monaten zahlreiche neue Arbeitsgruppen eingerichtet. Themen sind beispielsweise maschinelles Lernen, Quantencomputer sowie Informationssicherheit bei der Entwicklung und dem Aufbau des 5G-Mobilfunkstandards. (ur@ix.de)

Digitale Hinterlassenschaften prüfen

Neu auf der it-sa und am deutschen Markt zeigt sich das niederländische Unternehmen Cybersprint. Das 2015 gegründete Unternehmen ist auf das Scannen des „digitalen Fingerabdrucks“ von Unternehmen spezialisiert, also auf alles, was „von außen“ über das betreffende Unternehmen zu erfahren ist. Dazu gehören Informationen aus dem Web, aus den sozialen Medien, dem lokalen Netzwerk, mobilen Apps, dem Internet der Dinge sowie dem Dark Web. (Bei Dark-Web-Seiten sammelt das Tool alle verfügbaren Daten zunächst ein und durchsucht sie anschließend offline nach Unternehmensnamen und Stichwörtern. Das Suchen nach Klarnamen über die Suchfunktionen des Dark Web würde Verdacht erregen.) Auf diese Weise kann die Digital Risk Monitoring Platform etwa eine Schatten-IT oder Phishing-Websites entdecken, nicht genehmigte oder gefälschte Apps identifizieren, Schwachstellen finden und vieles mehr. Die Ergebnisse der Scans, die sich visuell aufbereiten lassen, führen zu einer Risikoeinschätzung, aufgrund derer sich die aufgedeckten Bedrohungen und Sicherheitslücken beseitigen lassen. (ur@ix.de)

Sophos schützt nun auch den Server

Nach Intercept X für Endpoints bringt Sophos das Produkt nun auch für Server heraus. Es beinhaltet Predictive Deep Learning, das nach der Übernahme von Invincea in die Intercept-X-Produkte integriert wurde. Die Engine wurde mit vielen Millionen Malware-Samples trainiert, die Sophos im Laufe der Jahre gesammelt hat, um nach eigenen Angaben mit geringer Fehlalarmrate sofort beim Anwender verdächtige von harmloser Aktivität unterscheiden zu können. Zudem soll das Produkt Angriffe auf Server vereiteln, selbst wenn die Systeme nicht gepatcht sind. Dazu kommt ein erweiterter Exploit-Schutz zum Einsatz auf Basis bekannter Exploit-Techniken in Kombination mit sogenannter Active Adversary Mitigation und Cloud-Workload-Erkennung. Ersteres beinhaltet neue Features zum Stören aktiver Angreifer, etwa das Verhindern des Diebstahls von Authentifizierungspasswörtern sowie Hash-Informationen aus dem Speicher, der Registry oder der Hard Disk oder Schutz vor Missbrauch von APIs. Des Weiteren soll WipeGuard verhindern, dass Ransomware den Master Boot Record (MBR) verschlüsselt.

Susanne Franke (ur@ix.de)

Bitdefender überarbeitet EDR-Modul

Bitdefender stellte eine neue Version seiner Endpoint Protection Platform (EPP) vor. GravityZone Ultra 3.0 hat mehr Funktionen in seinen Agenten gelegt. Zum erweiterten Funktionsumfang der neuen Version des EDR-Auswertungsmoduls (Endpoint Detection and Response) gehören Pre- und Post-Compromise-Forensik, intelligente Bewertung verdächtiger Aktivitäten, Visualisierung der Angriffstechniken, Echtzeitanzeige von IoCs (Indicators of Compromise) und automatisierte Problembehebung. Die Informationen zu den Einzelheiten der Vorfälle oder Angriffe sollen für Administratoren verständlicher und übersichtlicher sowie granularer visualisiert werden mit Timeline, Prozessstruktur und anderen Details. Ein Scoring klassifiziert zusätzlich alle Vorfälle nach Relevanz. Das Produkt verbindet vorbeugende Kontrollinstanzen und Erkennungstechnologien wie konfigurierbares Machine Learning, Verhaltensanalysen, Anti-Exploit sowie integriertes Sandboxing, um ausgeklügelte dateibasierte und dateilose Bedrohungen unterbinden zu können. Zu den nach eigenen Angaben wichtigsten neuen Features gehören dabei Mechanismen der „On-Execution Detection“, die Angriffe durch Überwachen des Arbeitsspeichers erkennen und sofort unterbrechen.

Susanne Franke (ur@ix.de)

Alle Links: ix.de/ix1811010