



**art of defence**, einziger deutscher Hersteller einer Web Application Firewall, bietet jetzt ein komplettes Produktpaket für den Schutz von Webapplikationen an. Die Produkte decken den Lebenszyklus einer Applikation, von Entwicklung über Qualitätssicherung bis hin zum Betrieb lückenlos ab. Alle Produkte sind aufeinander abgestimmt und die Ergebnisse eines Tools können automatisiert von den anderen Tools übernommen, ergänzt und verwertet werden.



Das erste Produkt, das Sourcecode-Analyse Tool *hypersource*, unterstützt Softwareentwickler und IT-Sicherheitsexperten bei der Entwicklung sicherer Webapplikationen. *hypersource* durchsucht den gesamten Quellcode nach potentiellen Schwachstellen und klassifiziert diese. So zeigt das Tool dem Nutzer beispielsweise kritische Schwachstellen direkt im Quellcode und unterstützt die Fehlerbehebung durch ausführliche und verständliche Erläuterungen. Dadurch und durch die Möglichkeit, *hypersource* direkt als Plugin in eine Entwicklungsumgebung zu integrieren, lernen Softwareentwickler Fehler zu vermeiden und somit effizienter zu arbeiten.

Die Ergebnisse einer Sourcecode-Analyse können vom Vulnerability Scan Server *hyperscan* übernommen und die mittels statischer Analyse gefundenen Schwachstellen mit Methoden der dynamischen Analyse auf praktische Ausnutzbarkeit überprüft werden. Anders als bei der Sourcecode-Analyse wird für einen Vulnerability-Scan kein Zugriff auf den Quellcode, sondern lediglich die URL der zu überprüfenden Webapplikation benötigt. Damit ist auch eine Schwachstellenanalyse von gekaufter und Open Source Software möglich. Die Analyse durch *hyperscan* erfolgt vollständig automatisiert. Auch diese Ergebnisse werden priorisiert und erläutert, so dass eine rasche und effiziente Fehlerbehebung ermöglicht wird.

Zur sofortigen Absicherung einer Webapplikation können die von *hypersource* und *hyperscan* entdeckten Schwachstellen direkt von der Web Application Firewall *hyperguard* geschlossen werden. *hyperguard* erstellt dazu auf Basis der Schwachstellenanalyse ein kompaktes aber verständliches Regelwerk, das die Webapplikation gezielt bis zur Produktivsetzung eines Patches schützt. Diese Möglichkeit ist besonders wichtig bei Schwachstellen, für die bereits Exploits kursieren, der Hersteller aber noch keinen Patch geliefert hat oder zur Vermeidung hektischer Notfalldeployments, die nicht ausreichend qualitätsgesichert werden konnten.

Alle drei Tools können, je nach konkretem Bedarf, auch eigenständig eingesetzt werden. Zusammen oder einzeln versetzen sie in die Lage, unternehmenskritische Daten vor Angreifern aus dem Internet zu sichern und die Verfügbarkeit der Webpräsenz zu gewährleisten. Sicherheitsstandards wie ISO27001 und PCI DSS können erst mit Hilfe solcher hochautomatisierten und ergonomischen Tools zu vertretbaren Kosten erreicht werden.

Die Suite an Tools ist ab sofort bei Computer & Competence erhältlich.