CyCognito-Studie: Webanwendungen sind großes Risiko für Unternehmen

Webapplikationen, die persönliche Informationen verarbeiten, sind oft nicht ausreichend vor Angriffen geschützt -- Konsequentes Risikomanagement als Basis zum Priorisieren und Beheben wichtiger Schwachstellen in der externen Cyber-Angriffsfläche

PALO ALTO, 21. September 2023 --- Webanwendungen gehören zu den größten Sicherheitsrisiken der externen Cyber-Angriffsfläche von Unternehmen - und sind trotzdem viel zu oft nicht ausreichend geschützt. Das ist ein zentrales Ergebnis des State of External Exposure Management Report von CyCognito, Marktführer für External Attack Surface Risk Management (EASM). Im Rahmen der Studie wurden zwischen Juni 2022 und Mai 2023 3,5 Millionen über das Internet erreichbare Assets wie Zertifikate, Domänen, Webserver, API-Endpunkte und Web-Apps auf Schwachstellen untersucht. Dabei wiesen 70 Prozent eklatante Sicherheitslücken auf, und knapp drei Viertel der Anwendungen, die persönliche Informationen (PII) wie Klarnamen, Mailadresse, Kontodaten oder Passnummern verarbeiten, waren mindestens einer gefährlichen und öffentlich bekannten - aber vom Unternehmen bisher nicht behobenen - Schwachstelle ausgesetzt. Zehn Prozent dieser Apps enthielten sogar eine für Angreifer leicht auszunutzende Lücke.

Von der äußeren Cyber-Angriffsfläche geht für Unternehmen ein hohes Risiko aus. Um dieses effektiv zu minimieren, empfiehlt der Report, neben regelmäßigen Überprüfungen die betroffenen Assets im Sinne eines konsequenten Risikomanagements im individuellen Kontext zu betrachten und entsprechend einzustufen, anstatt ausschließlich auf allgemeine Bewertungssysteme wie das Common Vulnerability Scoring System (CVSS) zu setzen. Denn nicht jede Sicherheitslücke birgt für jedes Unternehmen die gleiche Gefahr.

Web-Apps: Unzureichender Schutz für leicht ausnutzbare Ziele

Web-Apps machen 22 Prozent der typischen externen Cyber-Angriffsfläche aus und mindestens 30 Prozent von ihnen enthalten Sicherheitslücken. Webapplikationen werden oft zur Kommunikation mit Endkunden genutzt und stellen somit ein lohnendes Ziel für Cyberangriffe dar. Denn solche Apps arbeiten häufig mit wertvollen personenbezogenen Daten und sind nicht nur anfällig für Fehlkonfigurationen, sondern auch für Zero-Day-Exploits. Dass das von diesen Anwendungen ausgehende Risiko stark unterschätzt wird, zeigen die Zahlen des Reports: Fast ein Drittel der untersuchten Web-Apps nutzen für die Kommunikation kein HTTPS-Protokoll, 70 Prozent wurden nicht von einer Web Application Firewall (WAF) geschützt, und 25 Prozent nutzten weder HTTPS noch eine WAF.

Externe Angriffsfläche ist schwer zu managen

Die durch mit dem Internet verbundene Assets entstehende äußere Cyber-Angriffsfläche von Unternehmen ist dynamisch und ständigen Änderungen unterworfen. Eine große Fluktuation aktiver und genutzter Assets von etwa zehn Prozent im Monat erschwert es Unternehmen, einen Überblick zu behalten und die Bedrohungslage realistisch einzuschätzen. So ging ein Unternehmen von einem jährlichen Wachstum seiner äußeren Cyber-Angriffsfläche von drei Prozent aus, tatsächlich waren es 20 Prozent. Erschwert werden der Überblick und ein effektives Risikomanagement außerdem mit der Anzahl angegliederter Tochtergesellschaften. So fand eine frühere Studie von CyCognito heraus, dass 56 Prozent der kritischen und hochsensiblen Schwachstellen in der äußeren Angriffsfläche über Assets in Unterorganisationen entstehen.

Auf den individuellen Kontext kommt es an

Um ein Risikomanagement der externen Cyber-Angriffsfläche auch unter komplexen Voraussetzungen möglichst effizient betreiben zu können, gibt die Studie CI(S)Os einige Empfehlungen an die Hand. So sollten Security-Teams nicht nur besonders gefährdete Assets priorisieren, sondern untersuchen, welche bekannten Sicherheitslücken im unternehmenseigenen Kontext möglicherweise gar nicht so schwer wiegen - und die betroffenen Assets entsprechend depriorisieren. Denn nicht immer sind die von offiziellen Standards wie CVSS bewerteten Schwachstellen für die eigene Organisation tatsächlich so gravierend, wie der offizielle Score vermuten lässt. Der State of External Exposure Management Report zeigt: Von den Assets, die in einen Kontext gesetzt wurden, der unter anderem auch Verhaltensmuster von Angreifern berücksichtigt, konnten 35 Prozent trotz eines hohen CVSS-Scores als weniger kritisch eingestuft werden. Eine klare Priorisierung hilft Unternehmen, mit ihren begrenzten IT-Sicherheitsressourcen hauszuhalten und ihre individuell bedeutendsten Schwachstellen zuerst schließen zu können.

"Die externe Angriffsfläche eines Unternehmens verändert sich ständig, und diese Fluktuationen machen ein effektives Risikomanagement zu einer enormen Herausforderung", erklärt Dr. Georg Hess, Regional Sales Director bei CyCognito. "Vor allem Web-Apps sind für Angreifer ein lohnendes und oftmals einfach auszunutzendes Ziel. Um zu verhindern, dass sie zum Einfallstor werden können, sollten Organisationen neben regelmäßigen Tests auch eine individuelle, kontextbezogene Bewertung bekannter Schwachstellen für die eigenen IT-Systeme vornehmen - idealweise unterstützt von einer zentralen Plattform, die mit umfassenden Automatisierungskapazitäten Risiken aufdeckt und konsequent priorisiert."

Der gesamte State of External Exposure Management Report steht unter diesem Link kostenlos zum Download zur Verfügung: https://www.cycognito.com/resources/analyst-report/cycognito-state-of-external-exposure-management-report

Pressekontakt

Dr. Haffa & Partner GmbH

Herr Philipp Moritz
Karlstraße 42
80333 München

haffapartner.de
postbox@haffapartner.de

Firmenkontakt

CyCognito

Herr Dr. Georg Hess
Karlstraße 42
80333 München

https://cycognito.com
CyCognito@haffapartner.de

Über CyCognito
CyCognito ist Marktführer bei External Attack Surface Risk Management (EASM) und zählt viele Fortune-2000-Unternehmen zu seinen Kunden. Von der CyCognito-Plattform profitieren aber nicht nur große Unternehmen und Konzerne, sondern auch der Mittelstand. Die Plattform erlaubt ein proaktives, kontinuierliches Management der potenziellen Angriffsfläche, die ein Unternehmen über seine mit dem Internet verbundenen Assets bietet, und hilft, die damit verbundenen Risiken zu steuern und zu minimieren.
Kontinuierliches Monitoring inklusive einem weitreichendem automatisiertem Security Testing - ohne Input seitens des Kunden - zeigt regelmäßig die jeweils vollständige Angriffsfläche einschließlich "blinder Flecken" auf. Dazu gehören beispielsweise vergessene Cloud-Assets und nicht mehr genutzte oder fehlerhaft konfigurierte IT/IoT-Infrastrukturen. Das ist jedoch nicht alles: Dank relevanter Priorisierung und umfassender Integration in bestehende Security-Prozesse und -Plattformen (SOC, SIEM, SOAR, Ticketing-Systeme) können Unternehmen mit CyCognito effektiv jeweils die zehn Security-Lücken schließen, die 90 Prozent des gesamten externen Cyber-Risikos ausmachen.

Der Hauptsitz des Unternehmens ist heute in Palo Alto. Ursprünglich stammt CyCognito aus Israel, wo sich unter anderem die R&D-Abteilung befindet.

https//www.cycognito.com

Anlage: Bild


CYCOGNITO
SUMMER 2023 EDITION
Web Apps are Leaving PII Exposed
State of External Exposure Management Report