Papers AG

03.06.2026 – 14:09 Uhr

Innovative Schweizer Sicherheitstechnologie gegen globale Cyberbedrohungen: Papers AG lanciert "Obsidio" für hochrealistische DDoS-Resilienztests

Zug Schweiz (ots) -

Vor dem Hintergrund wachsender globaler Cyberbedrohungen und der zunehmenden Verwundbarkeit kritischer digitaler Infrastrukturen führt das Zuger Softwareunternehmen Papers AG die in ihrer Art einzigartige Sicherheitslösung Obsidio im Markt ein. Die bereits von renommierten Banken eingesetzte Lösung ermöglicht es Finanzinstitutionen und Betreibern kritischer Infrastrukturen, ihre Widerstandsfähigkeit gegen Cyberangriffe proaktiv, realistisch und laufend auf Herz und Nieren zu überprüfen, anstatt erst im Ernstfall zu reagieren. Die neue Applikation ist gezielt auf die Erfüllung der von den schweizerischen und europäischen Aufsichtsbehörden geforderten Nachweispflichten ausgerichtet.

Proaktiver Schutz in Zeiten drastisch zunehmender Cyber-Attacken

Herkömmliche Sicherheitstests stossen oft an ihre Grenzen, da sie Angriffe lediglich in künstlichen Laborumgebungen simulieren. Obsidio hingegen nutzt eine weltweit verteilte Infrastruktur von derzeit über 232'000 Smartphones, um realistische Überlastungsangriffe (Distributed Denial of Service, kurz DDoS) exakt nachzubilden. Bei einem DDoS-Angriff wird ein System durch eine massive Anzahl gleichzeitiger Anfragen lahmgelegt - vergleichbar mit tausenden Menschen, die gleichzeitig den Eingang eines Gebäudes blockieren.*

Digitale Souveränität und "Swissness" als Kernprinzip

Gerade für die Schweiz, deren Sicherheit immer weniger isoliert vom internationalen Technologie- und Cyberrisikoumfeld betrachtet werden kann, schafft Obsidio einen praxisnahen Ansatz zur Stärkung der digitalen Resilienz kritischer Systeme. Als in Zug ansässiges, renommiertes Tech-Powerhouse setzt die Papers AG auf Schweizer Ingenieurskunst und höchste Datenschutzstandards:

- **Dezentrale Sicherheit:** Durch die Nutzung der von der Papers AG entwickelten Acurast-Plattform, die verteilte Rechenleistung auf zehntausende reale Geräte
- weltweit verlagert, vermeidet Obsidio die Abhängigkeit von grossen, zentralen Cloud-Anbietern und reduziert systemische Risiken.
- **NSA-Immunität:** Dank der Verarbeitung in gesicherten Hardware-Bereichen der Mobilgeräte ist die Infrastruktur strukturell gegen unberechtigte externe Zugriffe und extraterritoriale Kontrolle geschützt.
- **Datenschutz:** Das System arbeitet nach strikten Zero-Trust-Prinzipien, ist vollständig DSGVO-konform und schützt die Privatsphäre aller beteiligten Nutzer durch deren ausdrückliche Zustimmung (Opt-in).

Erfüllung regulatorischer Anforderungen (FINMA & DORA)

Für Schweizer Banken und Versicherungen ist der Nachweis der operationalen Resilienz heute eine regulatorische Notwendigkeit. Obsidio liefert hierzu kryptografisch signierte und manipulationssichere Protokolle, die als Nachweis für Audits dienen. Durch die Bereitstellung aussagekräftiger Testergebnisse liefert die Plattform einen zentralen Nachweis der betrieblichen Widerstandsfähigkeit, der gezielt darauf ausgerichtet ist den Nachweispflichten gemäss FINMA (Schweizer Finanzmarktaufsicht), DORA (EU Digital Operational Resilience Act) und NIS2 (EU Digital Operational Resilience Act 2) nachzukommen.

"In einer Zeit, in der das Vertrauen in digitale Instrumente das höchste Gut darstellt, bietet Obsidio eine einzigartige Plattform, die dieses Vertrauen durch messbare Widerstandsfähigkeit untermauert", sagt **Alessandro de Carli**, CEO der Papers AG. "Obsidio transformiert das Cyber-Resilienz-Management von einer reaktiven Schadensbegrenzung hin zu einer proaktiven Überprüfung der Verteidigungssysteme."

***Hintergrund: Was ist eine DDoS-Attacke?** Eine DDoS-Attacke (Distributed Denial of Service) ist ein Cyberangriff, bei dem sehr viele Geräte oder Server gleichzeitig künstlich Anfragen an eine Website, Plattform oder digitale Infrastruktur senden. Das Ziel ist, das System zu überlasten, sodass es für echte Nutzerinnen und Nutzer langsam wird, ausfällt oder gar nicht mehr erreichbar ist. Für Banken, Behörden, Telekommunikationsanbieter, Spitäler oder andere kritische Infrastrukturen können solche Angriffe erhebliche operative, finanzielle und reputative Schäden verursachen.*

In der Schweiz und in Europa bleibt DDoS das bevorzugte Instrument für Hacktivisten, wobei diese Angriffe in der Schweiz alleine bereits 13 % aller Attacken auf kritische Infrastrukturen wie die öffentliche Verwaltung und den Finanzsektor ausmachen. Angesichts eines weltweiten Anstiegs der Angriffe um 168 % und massiver Traffic-Fluten von bis zu 31,4 Tbps ist auch die Schweizer Wirtschaft mit einer massiv verschärften Bedrohungslage konfrontiert. Da herkömmliche Schutzsysteme gegen neue KI-gestützte Botnetze zunehmend wirkungslos sind, drohen hiesigen Unternehmen bei schweren Angriffen mittlerweile finanzielle Schäden von fast 500'000 USD.

Über Obsidio

Obsidio ist eine "Swiss-engineered resilience testing platform", die spezifisch für kritische Infrastrukturen entwickelt wurde, Die Plattform ermöglicht realistische, dezentralisierte Simulationen, welche die Dynamik echter Cyberangriffe exakt widerspiegeln. Vor dem Hintergrund wachsender globaler Cyberbedrohungen und der zunehmenden Verwundbarkeit kritischer digitaler Infrastrukturen bietet Obsidio Organisationen die Möglichkeit, ihre Widerstandsfähigkeit nicht erst im Ernstfall, sondern kontrolliert, realistisch und proaktiv zu überprüfen. Die von der in Zug ansässigen Papers AG entwickelte Applikation ermöglicht maximale Ausfallsicherheit für kritischen Kommunikationsumgebungen und wird häufig von namhaften Finanzinstitutionen eingesetzt.

Obsidio bietet exklusiv fortschrittliche DDoS-Resilienz-Lösungen (Distributed Denial of Service), die es Organisationen ermöglichen, von einer reaktiven Schadensbegrenzung zu einem proaktiven Schwachstellen- und Vulnerabilitätsmanagement überzugehen. Mittels Integration des dezentralen Cloud-Computing-Protokolls **Acurast** definiert Obsidio die Standards für Sicherheit und Zensurresistenz neu. Acurast adressiert das Kernproblem der Zentralisierung, Ineffizienz und Fragilität traditioneller Cloud-Computing-Infrastrukturen, die massive Kapitalausgaben erfordern. Das Protokoll verwandelt ungenutzte oder ausrangierte Smartphones in eine globale, dezentrale Mesh-Cloud aus verifizierbaren und vertraulichen Compute-Providern. Durch die Simulation eines realistischen Botnetzes lassen sich mittels Obsidio Schwachstellen aufdecken, was mit den auf dem Markt verfügbaren zentralisierten Anbietern nicht möglich wäre. Obsidio nutzt dieses aus ethisch unbedenklichen Quellen stammende Botnetz, um realistische Angriffe durchzuführen. Durch den Standort Zug nutzt Obsidio die

regulatorische Klarheit und technologische Qualität des führenden Schweizer Technologie Standorts. Die Infrastruktur folgt strikten **Zero-Trust-Prinzipien** und ist durch die Dezentralisierung vollständig unabhängig von grossen, zentralisierten Cloud-Providern. Durch die präzise Simulation solcher Angriffe mittels eines realistischen Botnetzes lassen sich Schwachstellen aufdecken, die mit dem Markt verfügbaren zentralisierten Anbietern nicht aufgedeckt werden könnten. https://obsidio.com/de/

Über die Papers AG

Die Papers AG ist ein führendes Schweizer Softwareunternehmen mit Sitz in Zug, das sich seit über einem Jahrzehnt auf die Entwicklung von sicherer Blockchain-Infrastruktur und mobilen Sicherheitslösungen spezialisiert hat. Das Unternehmen entwickelt Schweizer Sicherheitstechnologie für eine Zeit, in der Cyberresilienz, digitale Souveränität und der Schutz kritischer Infrastrukturen zu zentralen strategischen Herausforderungen geworden sind.

Als global tätiges Tech-Powerhouse transformiert das ein Team hochkarätiger Spezialisten komplexe Technologien in benutzerfreundliche Open-Source-Anwendungen und hochsichere Enterprise-Software. Als Schweizer Unternehmen verbindet die Papers AG innovative "Swiss Made"-Ingenieurskunst mit strengsten Datenschutzstandards, um kritische Infrastrukturen abzusichern und die nächste Generation des digitalen Eigentums zu gestalten. https://papers.ch

Pressekontakte:

Nicky van der Eem, Papers AG, Baarer Strasse 43, CH-6300 Zug, Mail: n.vandereem@papers.ch,
Phone: +41 78 2560727

Peter Zimmermann, Managing Partner, Huber & Partner PR AG Switzerland, Probsteistrasse 95, CH-8051 Zurich, Phone +41 (0) 44 385 99 99, Fax +41 (0) 44 385 99 95, Mail: peter.zimmermann@huber-partner.com, web: www.huber-partner.com

Medieninhalte

Alessandro De Carli, CEO Papers AG / Weiterer Text über ots und www.presseportal.ch/de/nr/100103689 / Die Verwendung dieses Bildes für redaktionelle Zwecke ist unter Beachtung aller mitgeteilten Nutzungsbedingungen zulässig und dann auch honorarfrei. Veröffentlichung ausschließlich mit Bildrechte-Hinweis.