Fraunhofer SIT und Arkoon Netasq kooperieren für besseren Schutz vor Advanced Persistent Threats

Neuer Hash Guard Proof of Concept zeigt, wie eine der gefährlichsten Netzwerk-Sicherheitslücken unschädlich gemacht werden kann
Fraunhofer SIT zeigt Proototyp auf it-sa in Nürnberg

(Mynewsdesk) Das Fraunhofer-Institut für Sichere Informationstechnologie SIT und die Tochtergesellschaft von Airbus Defence and Space, Arkoon Netasq, zwei führende europäische Organisationen im Bereich Cybersicherheit, haben gemeinsam Hash Guard entwickelt, ein Proof of Concept, der Unternehmen vor den Folgen weit verbreiteter Pass-The-Hash-Angriffe schützt. Die Entwicklung ist Teil einer neuen Partnerschaft. Hacker verwenden Pass-The-Hash-Techniken, um Server-Authentifizierungen zu umgehen und sich Zugang zu geheimen Informationen und sensiblen Anwendungen zu verschaffen.

?Durch diese Zusammenarbeit haben wir erfolgreich ein Proof of Concept erfolgreich realisiert, das zurzeit mit wichtigen Kunden auf unserer Netzwerksicherheits-Plattform getestet wird?, sagt François Lavaste, Vorstandsvorsitzender von Arkoon Netasq. ?Unser Unternehmen ist bereits ein Pionier in der Bekämpfung von Pass-the-Hash-Angriffen dank unserer Stormshield Endpoint-Sicherheitslösung. Dieser netzwerkbasierte Schutz ist dafür eine perfekte Ergänzung und wird uns helfen, eine umfassende Lösung anzubieten.?
?Wir sind sehr glücklich über diese Partnerschaft, die einen führenden Anbieter von IT-Security-Lösungen mit einer der größten europäischen Forschungseinrichtungen verbindet?, sagt Michael Waidner, Leiter des Fraunhofer SIT. ?Das Ergebnis dieser Kooperation ist Hash Guard, ein effektiver Baustein, um Spionage und APTs einzudämmen. Er ist einfach zu implementieren und verbindet hohe Sicherheit mit Benutzerfreundlichkeit.?
Jedes Mal, wenn sich ein Benutzer an einem Windows-Netzwerk anmeldet, wird sein Passwort genutzt, um daraus eine Reihe von Sicherheitstokens zu erzeugen. Diese Hashes werden verwendet, um den Computer des Nutzers mit verschiedenen Servern und Anwendungen innerhalb des Firmennetzwerks zu verbinden. Aufgrund des Designs der Windows-Single-Sign-On-Authentifizierung fehlt ein Mechanismus, der sicherstellt, dass ein Hash ausschließlich von seinem rechtmäßigen Besitzer genutzt wird. Folglich können Angreifer Hashes stehlen und sie nutzen, um Zugang zu sensiblen Bereichen der Unternehmens-IT-Infrastruktur zu bekommen, wertvolle Informationen zu stehlen oder Kontrolle über das Netzwerk zu erlangen.
Hash Guard liefert diesen fehlenden Schutzmechanismus: Ähnlich wie eine Firewall ist Hash Guard den Unternehmensservern vorgelagert und überwacht dort Authentifizierungsnachrichten im Netzwerkverkehr. Hash Guard überprüft, ob ein Hash vom rechtmäßigen Eigentümer verwendet wird ? andernfalls trennt er automatisch sofort die Verbindung. Der Prototyp unterstützt Authentifizierung über Smartcards, wobei der Nutzer lediglich beim Einloggen seine PIN eingeben muss. Von da an überprüft Hash Guard regelmäßig eingehende Verbindungsanfragen zu den Servern. Hash Guard gewährleistet die Legitimität einer Verbindung, indem er sicherstellt, dass die Smartcard des Benutzers am anfragenden Rechner eingesteckt ist.
Hash Guard schützt Protokolle, die bei der LAN Manager- (LM) oder NT LAN Manager- (NTLM) Authentifizierungen zum Einsatz kommen, einschließlich des Server Message Blocks, (SMB), sowie zukünftig Internet Message Access Protocol (IMAP), Simple Mails Transfer Protocol (SMTP) und mehr. Eine Anpassung dieser Protokolle ist nicht erforderlich.

Über das Fraunhofer SIT
Das Fraunhofer-Institut für Sichere Informationstechnologie SIT ist einer der weltweit führenden Experten für Forschung und Entwicklung im Bereich Cybersicherheit. Das Institut ist in allen wichtigen Bereichen der IT-Sicherheit aktiv und bildet eine breite Basis von Kompetenz für technologieübergreifende Entwicklungen auf höchstem Niveau. Das Fraunhofer SIT bietet Dienstleistungen für alle Bereiche der Industrie. Zahlreiche erfolgreiche Projekte auf internationaler Ebene demonstrieren die Vertrauenswürdigkeit und Zuverlässigkeit des Fraunhofer SIT als Kooperationspartner.

Über Arkoon Netasq
Arkoon und Netasq sind hundertprozentige Tochtergesellschaften von Airbus Defence and Space. Sie führen die Marke Stormshield und verkaufen weltweit innovative Ende-zu-Ende-Sicherheitslösungen, um Netzwerke (Stormshield Network Security), Arbeitsplatzrechner (Stormshield Endpoint Security) und Daten (Stormshield Data Security)zu schützen.
Weitere Informationen finden Sie im Internet unter www.sit.fraunhofer.de

Shortlink zu dieser Pressemitteilung:
http://shortpr.com/59vk7p

Permanentlink zu dieser Pressemitteilung:
http://www.themenportal.
de/it-hightech/fraunhofer-sit-und-arkoon-netasq-kooperieren-fuer-besseren-schutz-vor-advanced-persistent-threats-76155

=== Hash Guard (Bild) ===

Hash Guard schützt Unternehmensnetze vor weitverbreiteten Angriffen.

Shortlink:
http://shortpr.com/8ewuvp

Permanentlink:
http://www.themenportal.de/bilder/hash-guard-26899

=== Hash Guard schützt Netzwerk vor weitverbreiteten Angriffen. (Infografik) ===

Hash Guard sorgt dafür, dass Passwort-Tokens auch wirklich nur vom Rechner des Benutzers genutzt werden können.

Shortlink:
http://shortpr.com/o6wspg

Permanentlink:
http://www.themenportal.de/infografiken/hash-guard-schuetzt-netzwerk-vor-weitverbreiteten-angriffen

Pressekontakt

Fraunhofer-Institut für Sichere Informationstechnologie

Herr Oliver Küch
Rheinstraße 75
64295 Darmstadt

presse@sit.fraunhofer.de

Firmenkontakt

Fraunhofer-Institut für Sichere Informationstechnologie

Herr Oliver Küch
Rheinstraße 75
64295 Darmstadt

sit.fraunhofer.de
presse@sit.fraunhofer.de

Die Informationstechnologie hat bereits weite Teile unseres Alltags durchdrungen: Ob Auto, Telefon oder Heizung ohne IT-Einsatz sind die meisten Geräte und Anlagen heute nicht mehr denkbar. Insbesondere Unternehmen nutzen ---IT-Systeme zur effektiven Gestaltung ihrer Arbeitsprozesse. Das Fraunhofer-Institut für Sichere Informationstechnologie beschäftigt sich mit dem Schutz dieser Systeme vor Ausfällen, Angriffen und Manipu-lationen.

Das Institut ist für Unternehmen aller Branchen tätig. Viele er-folg-reiche Projekte mit internationalen Partnern sind ein----drucks-voller Beweis für eine vertrauensvolle und zuverlässige Zusam-men--arbeit. Zu unseren Kunden zählen unter anderem die Deutsche Bank, SAP, Deutsche Telekom und das Bundesamt für Sicherheit in der Informationstechnik.