F5 Networks Studie: Onlinebedrohungen für Finanzdienstleister in EMEA-Region nehmen zu

? Ausmaß und Komplexität der Bedrohungen steigern Nachfrage nach Multi-Layer Web- und Mobile-Fraud-Erkennung und -Schutz

- Beträchtliche finanzielle Schäden bei fast jedem zweiten befragten Unternehmen in Deutschland, Frankreich, Großbritannien, Italien, Spanien, den Niederlanden, Schweden, Polen, den Vereinigten Arabischen Emiraten und Saudi Arabien in den vergangenen zwei Jahren

- Für 73 Prozent sind Reputationsschäden die größte Sorge

- Ausmaß und Komplexität der Bedrohungen steigern Nachfrage nach Multi-Layer Web- und Mobile-Fraud-Erkennung und -Schutz

- Große Unternehmen bevorzugen zunehmend hybride Lösungen

Edinburgh, 20. Mai 2015 - Finanzdienstleister in der EMEA-Region sind einer steigenden Zahl von Web-Fraud-Bedrohungen ausgesetzt. Das ist das Ergebnis einer aktuellen Studie von F5 Networks (NASDAQ: FFIV) in Deutschland, Frankreich, Großbritannien, Italien, Spanien, den Niederlanden, Schweden, Polen, den Vereinigten Arabischen Emiraten und Saudi Arabien[1]. Demnach verzeichneten in den vergangenen zwei Jahren 48 Prozent der befragten Unternehmen finanzielle Schäden von zwischen 50.000 und 500.000 britischen Pfund, neun Prozent von über 500.000 britischen Pfund und drei Prozent von über einer Million britischen Pfund aufgrund von Onlinebetrug. Die Studie deckt auf, welche Herausforderungen IT-Entscheider täglich bewältigen müssen, um finanzielle Schäden und Reputationsverluste aufgrund von Malware, Phishing, Credential Grabbing und Session-Hijacking-Attacken zu verhindern. Diese Herausforderungen führen zu einer steigenden Nachfrage nach Multi-Layer-Web-Fraud-Lösungen - auch für mobile Endgeräte.

73 Prozent der Befragten sorgen sich vor allem um ihre Reputation, 72 Prozent fürchten finanzielle Einbußen und den massiven Folgeaufwand durch umfangreiche Sicherheits-Audits. Weitere negative Auswirkungen von Web Fraud sind sinkende Kundenloyalität (64 Prozent) und von Aufsichtsbehörden verhängte Strafzahlungen (62 Prozent).

"Ob Phishing-Attacke, Man-in-the-Middle, Man-in-the-Browser oder trojanerbasierte Aktivitäten wie Web Injection, Form Hijacking, Page Modification und Transaktionsmodifizierungen - überall lauern Web-Fraud-Gefahren auf Unternehmen aller Branchen", erklärt Gad Elkin, EMEA Security Director bei F5 Networks.

"Mehr als je zuvor ist es unumgänglich, die Art der Bedrohungen zu verstehen, um geeignete Gegenmaßnahmen zu ergreifen, bevor ein wirklicher Schaden entsteht. Jetzt gilt es, die richtigen Entscheidungen zu treffen, um Kundentreue und Gewinne zu erhalten. Andernfalls riskieren Unternehmen das, was ihnen am wichtigsten ist - ihre Reputation."

Mehr als 35 Prozent der Befragten gaben an, bereits von Betrugsfällen durch verschiedene Online-Attacken betroffen gewesen zu sein. Malware ist dabei mit 75 Prozent der Hauptverursacher, gefolgt von Phishing (53 Prozent), Credential Grabbing (ebenfalls 53 Prozent) und Session Grabbing (35 Prozent).

Als Abwehrstrategie bevorzugen 37 Prozent aller Unternehmen einen Web-Fraud-Schutz mittels hybrider Lösungen, bestehend aus einer Kombination aus On- und Off-Premise-Lösungen. Das gilt insbesondere für große Unternehmen mit mehr als 5.000 Mitarbeitern (59 Prozent).

55 Prozent der Befragten nutzen Multi-Layer-Betrugspräventionslösungen. Endpoint Embedded Solutions sind mit 62 Prozent am beliebtesten, gefolgt von Page-Navigation-Analysen, die ungewöhnliche Navigationsmuster identifizieren (59 Prozent), und Entity-Link-Analysen von Beziehungen von Benutzern, Konten und Maschinen, um kriminelle Aktivitäten und Missbrauch (59 Prozent) zu erkennen. Lösungen für die Nutzerverhaltensanalyse und Vergleiche von spezifischen Kanälen werden von 55 Prozent verwendet.
Das meiste Budget fließt in Web Channel Fraud Protection (52 Prozent) und Mobile Fraud Protection (36 Prozent).

Vor diesem Hintergrund erklärt sich die wachsende Nachfrage nach Lösungen mit Funktionen für einen clientlosen Onlinebetrugsschutz. Damit können Unternehmen verschiedenste Endgeräte in Echtzeit gegen unterschiedlichste Webbedrohungen schützen, ohne dass der Anwender etwas tun müsste. Damit sind Endgeräte beispielsweise nicht mehr anfällig für schädlichen HTML-Code oder Script Injections - und auch nicht gegen Bedrohungen wie die Dyre Malware, einen der aktuell gefährlichsten Banking-Trojaner. "Betrüger entwickeln sich immer weiter und zielen auf das schwächste Glied: den Endanwender", erklärt Elkin.

"Beim Absichern von Rechenzentren, Multifaktor-Authentifizierung und dem server-seitigen Schutz von Applikationen sind Unternehmen schon sehr weit. Trotzdem ist der Endpunkt, an dem der Nutzer mit Webapplikationen interagiert, häufig nach wie vor nicht effektiv geschützt."

ca. 4.000 Zeichen mit Leerzeichen

[1]Die Studie wurde von IDG Connect (http://www.idgconnect.com) durchgeführt. Das Unternehmen hat über 100 IT-Entscheider bei Finanzdienstleistern mit mehr als 250 Angestellten in Deutschland, Frankreich, Großbritannien, Italien, Spanien, Niederlande, Schweden, Polen, Vereinigte Arabische Emirate und Saudi Arabien befragt.

Pressekontakt

Dr. Haffa & Partner GmbH

Herr Axel Schreiber
Burgauerstr. 117
81929 München

haffapartner.de
postbox@haffapartner.de

Firmenkontakt

F5 Networks

Frau Sibylle Greiser
Lehrer-Wirth-Straße 2
81829 München

f5.com/
s.greiser@f5.com

F5 (NASDAQ: FFIV) bietet Lösungen für eine Welt voller Applikationen. F5 unterstützt Unternehmen, Cloud-Systeme, Rechenzentren und Software Defined Networks (SDN) zu skalieren, um für jeden, jederzeit und überall Anwendungen optimal bereitzustellen. Die Lösungen von F5 erweitern die IT durch eine offene, skalierbare Struktur und unterstützen durch ein starkes Netzwerk aus Partnern und Allianzen der führenden Anbieter im Bereich Technologie- und Rechenzentren. Dieser Ansatz ermöglicht Kunden, eine Infrastruktur zu entwickeln, die zukünftigen Anforderungen gerecht wird. Führende Konzerne und internationale Unternehmen, Service Provider sowie Institutionen des öffentlichen Dienstes verlassen sich auf F5, wenn es um Cloud-, Security- und Mobility-Trends geht.

Weitere Informationen finden Sie auf http://www.f5.com/.

Folgen Sie F5 auf Twitter (https://twitter.com/F5networksde) oder besuchen Sie uns auf Facebook (http://www.facebook.com/f5networksinc), um mehr über F5, die Partner und Technologien zu erfahren.

Anlage: Bild