

Hacker von BT verbessern Datensicherheit in der Finanzbranche

Sicherheitstests von BT mit CREST STAR-Zertifizierung unterstützen Finanzinstitute bei der Abwehr von Cyber-Angriffen / Der Netzwerk- und IT-Dienstleister BT bietet ab sofort weltweit seinen neuen Sicherheits-Service „BT Assure Ethical Hacking for Finance“ an. Mit aufwändigen Testverfahren wird geprüft, in welchem Maße Finanzdienstleister durch Cyber-Angriffe gefährdet sind.

Finanzinstitute wie Banken und Versicherungsunternehmen verfügen über eine Vielzahl wertvoller und hoch sensibler Kundendaten, was sie zu einem der begehrtesten Ziele für Hacker und Cyberkriminelle macht. Das Risiko, Ziel eines Angriffs zu werden, ist in den vergangenen Jahren weiter gewachsen, da immer mehr Bankdienstleistungen online angeboten werden und Wertpapiere in verstärktem Maße über elektronische Plattformen gehandelt werden.

Assure Ethical Hacking for Finance nutzt erprobte Verfahren, die das Vorgehen krimineller Hacker und Angreifer nachahmen. Mit einer Reihe von Verfahren werden die Einstiegspunkte der bankeigenen IT-Systeme getestet sowie potenzielle Schwachstellen im Unternehmen aufgedeckt. Überprüft werden unter anderem Mobilgeräte und sonstige Hardware von Laptops bis hin zu Druckern, interne und externe Netzwerke, Datenbanken und komplexe ERP-Systeme. BT testet nicht nur Systeme mit Netzwerkzugriff, sondern prüft auch, wie groß das Risiko eines menschlichen Fehlers ist. So wird beispielsweise mithilfe von Social Engineering getestet, ob die Mitarbeiter die Sicherheitsrichtlinien einhalten und wie hoch zum Beispiel die Anfälligkeit für einen Phishing-Angriff ist.

Der neue Service beruht auf den Erfahrungen mit Ethical Hacking, die BT in Zusammenarbeit mit führenden Finanzinstituten über zwei Jahrzehnte gemacht hat. Innerhalb eines strikt definierten Auftrags konnten die ethischen Hacker von BT zahlreiche Schwachstellen aufdecken. So konnten sie unter anderem

- Auszüge aus Datenbanken mit zehntausenden von Sozialversicherungs- und Kreditkartennummern beschaffen
- eingereichte Schecks abfangen und manipulieren
- firmeneigene Verschlüsselungsverfahren durch „Reverse Engineering“ überwinden
- Wertkarten mit Guthaben von fremden (Test-)Konten aufladen
- sich mit Hilfe gefälschter E-Mails, die von arglosen Mitarbeitern geöffnet wurden, Administratorenrechte verschaffen
- Remote-Access-Verbindungen manipulieren, um Zugriff auf die Kommandoebene (Shell) von IT-Systemen zu bekommen und darüber eine direkte Verbindung (Tunnel) ins Unternehmensnetz aufzubauen
- Geldbeträge zwischen unautorisierten Testkonten transferieren
- vollständige Kontodaten für alle Nutzer abgreifen, indem sie die M2M-Kommunikation zwischen Backend-Systemen angriffen*.

Das übergeordnete Ziel dieser Tätigkeit besteht dabei immer darin, Schwachstellen zu identifizieren, die geschäftskritische Prozesse und somit auch das Ansehen und die Marke eines Unternehmens gefährden.

Im Rahmen von Assure Ethical Hacking for Finance nutzt BT CREST**-zertifizierte STAR-Services (Simulated Targeted Attack and Response), um Finanzdienstleister bei der Entwicklung zuverlässiger Sicherheitslösungen zu unterstützen, so dass sensible Kundendaten bestmöglich geschützt werden. BT wurde als eines der ersten Unternehmen weltweit von CREST für die Bereitstellung von STAR-Services akkreditiert.

CREST hat die STAR-Zertifizierung entwickelt, um kontrollierte, maßgeschneiderte und intelligente Testverfahren im Bereich Cybersicherheit zu etablieren. STAR wurde in Zusammenarbeit mit der Bank of England und der britischen Regierung konzipiert. Mithilfe fortschrittlicher Penetrationstests und umfassender Bedrohungsanalysen sollen die Cyber-Gefahren noch präziser simuliert werden.

Mark Hughes, President BT Security, sagte: „Vertrauliche Finanzdaten sind für viele Hacker ein lohnendes Ziel. Kaum ein Unternehmen ist deshalb so attraktiv für Cyberkriminelle wie eine Bank. Abgesehen von den unmittelbaren finanziellen Verlusten kann eine schwerwiegende Sicherheitsverletzung irreparable Imageschäden nach sich ziehen. Auch wenn vor allem Privatkundenbanken im Visier der Täter stehen, sind Investmentbanken ebenso betroffen wie auch Geschäftskunden-banken, die Dienstleistungen wie Währungsumrechnungen und Handelstransaktionen für große Geschäftskunden bereitstellen. Wir raten allen Finanzinstituten, rigorose Tests zur Prüfung der Sicherheitsstandards durchzuführen. Unsere Ethical Hacker gehen dabei bis an die Grenzen der Sicherheitssysteme, die in Finanzinstitutionen implementiert sind.“

BT verfügt über ein ausgezeichnetes internationales Team von Sicherheitsspezialisten. Dazu gehören auch Ethical Hacker, die mithilfe standardisierter Verfahren Systeme durch die Simulation von Hacker-Angriffen testen. Dabei werden Schwachstellen identifiziert und konkrete Korrekturmaßnahmen vorgeschlagen, damit die Kunden die betroffenen Anwendungen und Systeme innerhalb kürzester Zeit ausbessern können.

*Andere Beispiele aus der Praxis können Sie in unserer Fallstudie (http://www.globalservices.bt.com/uk/en/casestudy/international_financial_services_provider) nachlesen.

**CREST ist eine gemeinnützige Organisation im Bereich der technischen Informationssicherheit, die sich der Bereitstellung hochwertiger Professional Services verschrieben hat. Weitere Informationen finden Sie hier: <http://www.crest-approved.org/why-use-crest/index.html>