PRESSEMITTEILUNG

Cyberangriffe auf Geldautomaten nehmen seit Lockdown stark zu – Cybersicherheit ist für Banken wichtiger denn je

Élida Policastro, Regional VP - Cybersecurity Division bei Auriga,
zur aktuellen Lage der Cyberbedrohungen für Finanzinstitute
und was zum Schutz davor unverzichtbar ist

BARI, 27. Oktober 2020 - Cyberangriffe auf Geldautomaten und die dazugehörigen Infrastrukturen von Banken sind eine seit Jahren wachsende Gefahr für Finanzinstitute weltweit. Diese Gefahr hat sich für Banken in der ersten Hälfte dieses Jahresstark verschärft. Die Anzahl der Malware-Angriffe auf Banken und andere Finanzdienstleister hat in den ersten sechs Monaten des Jahres 2020 massiv zugenommen, wie die European Association for Secure Transaction (EAST) berichtet. Demzufolge ist die Zahl der Jackpotting- oder auch Black Box-Angriffe in diesem Zeitraum um 269 Prozent gestiegen – von 35 Angriffen im Vergleichszeitraum des Vorjahres auf 129 im ersten Halbjahr 2020. Verbundene finanzielle Verluste stiegen im gleichen Vergleich von unter 1.000 Euro auf über eine Million Euro. Seitens der Angreifer wurde darauf spekuliert, dass die Systemabwehr durch Home Office, Remote Access und der möglichen resultierenden Überlastung von Servern stark geschwächt ist. Somit ist es für Finanzinstitute derzeit besonders wichtig, eine effektive Strategie für Cybersicherheit zu implementieren, um ihre Geräte, ihr Kapital und ihre Kunden zu schützen.

Cyber-Angriffe auf Geldautomaten und die Systeme, die Geldautomaten steuern, wie z.B. zentrale Server, stellen weltweit eine akute und wachsende Bedrohung dar. Cyberangriffe können beispielsweise zum Diebstahl persönlicher Daten wie Kontonummern und PIN-Codes führen. Es ist jedoch für die Angreifer relativ aufwändig, diese Daten in Geld umzuwandeln. Sogenannte Jackpotting-Angriffe sind sehr beliebt, da sie im Erfolgsfall den Geldautomaten zur sofortigen Bargeldausgabe überlisten. Bei dieser Art von Angriffen werden physische oder softwarebasierte Schwachstellen genutzt, um auf das enthaltene Bargeld sowie die persönlichen Daten der Nutzer zugreifen zu können. Geldautomaten sind oft schlecht überwacht und es werden wenige logische Maßnahmen ergriffen, um die Sicherheit der Daten zu gewährleisten.

Das Ökosystem „Geldautomaten“ ist komplex, es besteht aus heterogener Hardware und Software und oftmals fehlen in den Organisationen proaktive Aktualisierungsrichtlinien und ein zentraler Überblick über die Sicherheitsstruktur.

Wirkungsvolle Mechanismen für lückenlosen Schutz
Um sicherzustellen, dass die Geräte einer Bank bestmöglich vor Cyberangriffen geschützt sind, sollte zunächst ein Sicherheitsexperte befragt werden, der die bestehenden Sicherheitspläne und -prozesse prüft und bewertet. Darüber hinaus ist es elementar wichtig, bei Mitarbeitern und Kunden ein Bewusstsein zu schaffen für die Gefahr, die von Cyberangriffen ausgeht und die Maßnahmen, die für effektive Cybersicherheit erforderlich sind.

Hinsichtlich Geldautomaten ist es nicht ausreichend, generische Schutztechnologie für die Endpunkte anzuwenden wie beispielsweise Anti-Malware-Lösungen. Geldautomaten stellen eine kritische Infrastruktur dar, die für einen Neustart nicht einfach ausgeschaltet werden kann. Die Geräte müssen rund um die Uhr und an 365 Tagen im Jahr verfügbar sein, sodass sie ein höheres Maß an Schutz und eine andere Herangehensweise an die Cybersicherheit erfordern. Banken brauchen eine zentralisierte Sicherheitslösung, die ihre Geldautomatennetzwerke schützt, überwacht und steuert. So sind sie in der Lage, ihr gesamtes Geldautomatennetzwerk an einem Ort zu verwalten, um Malware-Angriffe oder betrügerische Aktivitäten an gefährdeten Geldautomaten zu stoppen.

Eine integrale Geldautomaten-Sicherheitslösung, die eine zentrale Verwaltung des Geldautomatennetzwerks und eine Remote-Ausführung von Aktivitäten ermöglicht, spart Banken Zeit und Geld. Für Banken ist es essenziell, über mehrere Schutzebenen in einer einzigen Plattform zu verfügen. Das zeichnet auch die Geldautomaten-Cybersicherheitslösung Lookwise Device Manager (LDM) von Auriga besonders aus.

Finanzinstitutionen sind aufgrund ihrer hohen Vermögenswerte attraktive Ziele für Cyberangriffe. Die Mittel, mit denen Cyberangriffe ausgeübt werden, werden kontinuierlich weiterentwickelt und technologisch versierter. Daher müssen Banken stets auf dem neuesten Stand bleiben und einen proaktiven Ansatz zur Cybersicherheit verfolgen. Da dieses Thema in den kommenden Jahren an Relevanz gewinnen wird, sollten Finanzinstitute ihre Konzepte für Cybersicherheit konstant weiterentwickeln, um mit den Bedrohungen Schritt halten zu können.

Geschäftskontinuität im Fall eines erfolgreichen Cyberangriffs sichern
Aber auch für den Fall, dass ein Cyberangriff, zum Beispiel durch Ransomware, erfolgreich ist, sollte eine Bank im Rahmen eines ganzheitlichen operationellen Widerstandssystems ein wirksames Konzept zur Geschäftskontinuität erarbeiten. Mit einem solchen können im Katastrophenfall die betroffenen Daten und Systeme wiederhergestellt werden, während der Geschäftsbetrieb so wenig wie möglich beeinträchtigt wird.

Auriga - Taunusanlage 1 - Frankfurt 60329 - Tel: +49 69 50 50 60 702 - Fax: +49 69 50 50 60 520 - Stammkapital 1.196.055 €
www.aurigaspa.com - frankfurt@aurigaspa.com

Sollten Sie Interesse an einem Gespräch mit Élida Policastro haben, bringen wir Sie gerne in Kontakt.

Über Auriga:

Auriga ist einer der führenden Anbieter von Software und Anwendungslösungen für den Banken- und Zahlungsverkehrssektor und ein Experte für innovative Omni-Channel-Lösungen für Banken und andere Finanzinstitute. Dazu zählt ein breites Spektrum an Anwendungen und Dienstleistungen für die Entwicklung und das nahtlose Management von SB-Kanälen, virtuellem Banking und Bankfilialen.

Da Auriga kontinuierlich in Forschung und Entwicklung investiert und seine Software-Spezialisten mit Weitblick innovative, zuverlässige Lösungen erarbeiten, ist das Unternehmen heute ein Vorreiter bei flexiblen und modularen Anwendungen, die sich in die jeweiligen Backend-Systeme der Banken einbinden lassen. Aurigas Softwarelösungen, die bereits auf 70 Prozent aller italienischen (und 12% der europäischen) Bankautomaten laufen basieren somit auf moderner Architektur. Darüber hinaus verbessern sie die Markteinführungszeit von neuen Diensten enorm und bieten umfassende Funktionen zum Schutz, zur Überwachung und zur Steuerung von kritischen Geräten. Zudem senken sie die Kosten und verschaffen Finanzinstituten langfristig einen entscheidenden Wettbewerbsvorteil. Auriga ist ein globales Unternehmen mit Präsenzen in West- und Osteuropa, Lateinamerika und dem asiatisch-pazifischen Raum. Besuchen Sie für weitere Informationen www.aurigaspa.com/deu/, Twitter, LinkedIn oder XING.

Pressekontakt:
Allison + Partners
Aljona Jauk
Theresienstraße 43, 80333 München
Tel: +49 (0)89 388 892 015
E-Mail: aurigager@allisonpr.com