MARKET INSIGHT #4

Security Services für ATMs

AUF EINEN BLICK

Der Trend bei Bankenattacken geht hin zu logischen und Cyberangriffen.

Die Gefahr von Cyberattacken aus dem Banksystem heraus wird in Zukunft als neuer Angriffsvektor für ATMs an Bedeutung gewinnen.

Diese neue Bedrohungslage erfordert eine zentrale, bankenübergreifende Lösung. Zukünftig bietet der ATM Security Service von SIX als zentrale Anlaufstelle ATM-Alarmierung und Abwehrhinweise aus einer Hand.

ATMs: Veränderte Angriffsmuster

Spektakuläre Raubzüge auf Geldautomaten sind oft in den Medien. Tatsächlich ging die Anzahl physischer Attacken unter massiver Gewaltanwendung in der Schweiz zuletzt zurück, während «smartere» Angriffsformen, sog. logische Attacken, an Bedeutung gewinnen. So registrierte SIX im Jahr 2019 in der Schweiz 43 physische Angriffe, 2020 waren es nur noch 19. Das entspricht einem Rückgang von 56 %.

Im gleichen Zeitraum stieg die Zahl der logischen Attacken um 86 %. Auffällig dabei ist, dass sich die Art der von den Angreifern favorisierten logischen Attacken verändert. Der Anteil der Skimming-Attacken, bei denen durch technische Manipulation des Kartenlesers am Geldautomaten die Daten von Kredit- oder Bankkarten ausgespäht werden können, sinkt – in der Schweiz insbesondere durch das von SIX eingeführte Geoblocking. Die Zahl der Blackbox-Attacken hingegen steigt rasant – nicht nur in der Schweiz, sondern international. Bei diesem Angriffsmuster wird im Automaten ein kleiner Computer verbaut, über den Malware aufgespielt beziehungsweise logische Attacken durchgeführt werden. Die European Association for Secure Transactions (EAST) weist für Europa im ersten Halbjahr 2020 einen Anstieg von Blackbox-Attacken um 269 % aus.

Darüber hinaus spielt ein weiterer Angriffsvektor eine immer grössere Rolle: Cyberattacken auf ATM-Netzwerke, bei denen sich Hacker Zugang zu den IT-Netzwerken der Banken verschaffen und die Angriffe von dort heraus verüben.

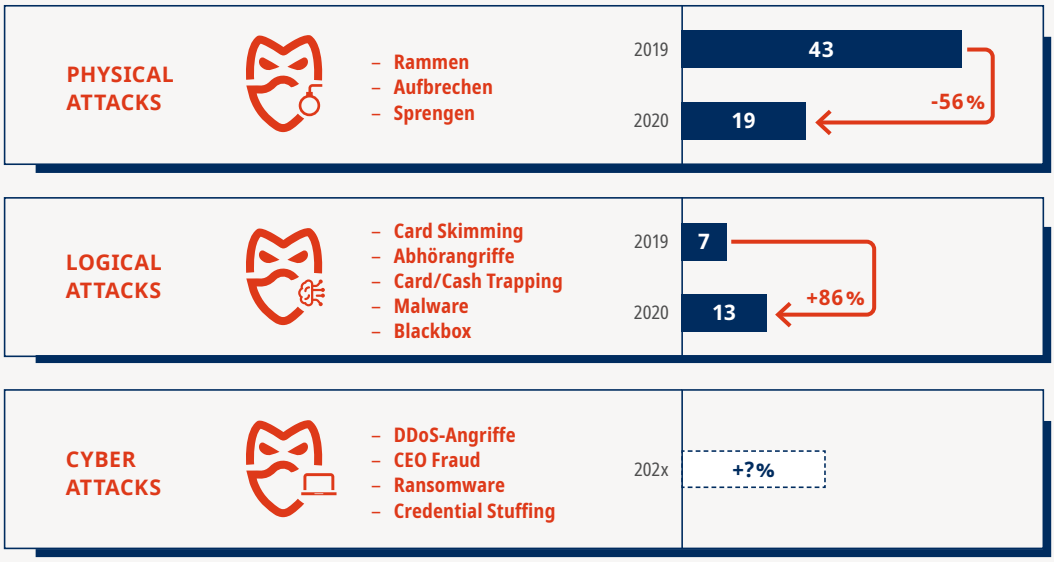

Abb. Veränderte Angriffsmuster auf ATMs in der Schweiz, Quelle: SIX

Herausforderung: Cyber Security

Cyber Security ist eine globale Herausforderung. Das zeigt nicht zuletzt die weltweite Cyberattacken-Welle, die seit März 2020 gegen Regierungsstellen, Telekommunikations- und Rohstoffunternehmen läuft und in deren Zuge im Dezember 2020 Hacker in die Computer des US-Handels- und Finanzministeriums eingedrungen sind. Keine Branche wird so stark angegriffen wie die Finanzbranche. «Organisierte Cyberkriminalität versucht Finanzinstitutionen in Geiselhaft zu nehmen und die digitale Transformation zu kapern», konstatiert der Cloud Provider VMware Carbon Black in seinem Sicherheitsbericht «Modern Bank Heists 2020». Demzufolge nahm im ersten Quartal 2020 die Anzahl der Cyberangriffe auf Banken um 238 % zu.

Es mag auf den ersten Blick beruhigen, dass der von SIX veröffentlichte Cyber Security Report 2020 für die Schweiz im Vergleich zu anderen Ländern nach wie vor eine sehr geringe Zahl von Cyberattacken ausweist. Dabei ist jedoch zu berücksichtigen, dass Meldungen über Cyberangriffe an die Melde- und Analysestelle Informationssicherung (MELANI), die dem Nationalen Zentrum für Cybersicherheit (NCSC) angegliedert ist, (noch) freiwillig geschehen.

Fakt ist: Cyberattacken auf Bankensysteme sind eine ernstzunehmende Bedrohung. Das gilt zunehmend auch für Geldautomaten.

Zukünftige Bedrohungslage für ATMs

Noch konzentrieren sich Hacker auf DDoS-Angriffe, wobei Kapazitäten zur Verarbeitung von Anfragen gezielt überschritten werden und so die Verfügbarkeit eines Zielsystems ausser Kraft gesetzt wird. Weiterhin kommen Betrugsmaschen wie CEO-Fraud-Attacken, Credential Stuffing – systematischer Missbrauch von Zugangsdaten – sowie Ransomware zum Einsatz, wobei bösartige Software durch Verschlüsselung den Datenzugriff verweigert. Es ist eine Frage der Zeit, wann Hacker ihren Zugang zu den Bankennetzwerken nicht nur zur Datenverschlüsselung und zum Datenraub nutzen, sondern über diesen Weg auch im grossen Massstab ATM-Netzwerke angreifen. Sie könnten ihre Schadsoftware nutzen, um Bargeldauszahlungen zu veranlassen und vor Ort abzuholen. Wenn dies gelingt, wird sich die Methode rasend schnell über den Globus verbreiten. Denn Hacker verbünden sich international und tauschen Know-how und Daten aus, um gemeinsam effektivere Angriffsmethoden zu entwickeln.

Schweizer Banken müssen sich der Bedrohung durch logische und Cyberattacken stellen. Es bedarf eines konzertierten, effizienten und wirkungsvollen Handelns aller ATM-Stakeholder, um ein Frühwarnsystem aufzubauen und koordinierte Abwehrmassnahmen zu entwickeln.

Sicherheitslage der Schweizer ATMs

Die aktuelle Situation der ATM-Sicherheit erfordert ein orchestriertes Handeln aller ATM-Stakeholder. Sämtliche Betreiber von ATM-Infrastrukturen sehen sich mit denselben Risiken und Bedrohungen konfrontiert. Doch es fehlt ein holistischer Blick auf alle Attacken. Dutzendfach wird gleichzeitig an Lösungen gearbeitet. Anstatt die Kräfte zu bündeln, überwachen mehrere Banken die gleichen Quellen parallel. Auch das kontinuierliche Lernen über Art und Weise der Angriffe geschieht aktuell nur individuell auf Ebene der einzelnen Finanzinstitute. Durch den Bedeutungsverlust des Bargeldes und damit der ATMs geht zudem wertvolles ATM-Wissen verloren, da Stellen nicht nachbesetzt werden.

Letztendlich fehlt eine zentral gesteuerte Kommunikation zwischen den ATM-Stakeholdern. Ausserdem mangelt es an einer Infrastruktur, über die sich Angriffswellen und ihre Methoden zeitnah und ganzheitlich erkennen lassen, über die der Verlauf von Attacken nachvollzogen werden kann und rechtzeitig vorausschauende Warnungen ausgesprochen bzw. wirksame Gegenmassnahmen ergriffen werden können.

Made in Switzerland: Der neue ATM Security Service

Die aktuellen und zukünftigen Bedrohungstrends haben Schweizer Banken gemeinsam mit SIX bereits 2018 in den Fokus genommen. Bankenübergreifende Workshops wurden initiiert, Sicherheitsvorfälle sowie Attacken analysiert. Einigkeit besteht, dass ein neuer zentraler ATM-Sicherheitsservice benötigt wird, um

- eine holistische Sicht auf Angriffe zu bekommen
- Risiken gezielt zu erkennen und entsprechende Massnahmen zu initiieren
- qualitativ hochwertige Reports zur Verfügung zu stellen
- eine zentrale Plattform für einheitliche Daten und Informationen bereitzustellen
- eine zentrale Anlaufstelle für alle Schweizer Banken zu etablieren
- eine institutionalisierte Alarmierungs- und Informationskette aufzubauen

Auf dieser Grundlage hat SIX mit dem Aufbau der ATM Security Services begonnen. Im Zuge des neuen Dienstleistungsangebots werden die ATM-Events, -Meldungen und -Alarme der beteiligten Banken zentral überwacht, Informationen von MELANI, EAST und anderen öffentlichen Quellen zu neuen Bedrohungen rund um Geldautomaten ausgewertet und Warnungen der Geldautomatenhersteller berücksichtigt.

Das zentrale ATM Security Framework von SIX wird ausgebaut und auf drei Säulen fussen:

THREAT INTELLIGENCE & SECURITY ADVISORY	SECURITY & EVENT ANALYSIS	ALARMING & RAPID RESPONSE
Zentrales Monitoring weltweiter Nachrichten zu neuen Vorgehensweisen und Bedrohungen von Bancomaten sowie regelmässige Informationen an die beteiligten Banken	*Zentrale Analyse zu Risikopotenzialen für Bancomaten in der Schweiz*	*Anlassbezogene Alarmierung und kontinuierliche Information sowie Bereitstellung von Handlungsempfehlungen für die beteiligten Banken*

WEITERE INFORMATIONEN HIER

SIX BBS AG
Hardturmstrasse 201
Postfach
8021 Zürich
T +41 58 399 4012
cash@six-group.com