MARKET INSIGHT #4

Security Services for ATMs

AT A GLANCE

The trend in attacks on financial institutions is shifting towards logical and cyber attacks.

The risk of cyber attacks from within the banking system will become increasingly significant as a new attack vector for ATMs in future.

This new threat level requires a central, cross-bank solution. In future, the ATM Security Service provided by SIX will offer ATM alarming and defense guidance from a single source.

ATMs: Changed Attack Patterns

Spectacular raids on ATMs are frequently reported in the media. In actual fact, the number of physical attacks involving massive use of force in Switzerland has been falling recently, while “smarter” forms of attack, known as logical attacks, are becoming more significant. Accordingly, SIX registered 43 physical attacks in Switzerland in 2019 as opposed to only 19 in 2020. This corresponds to a fall of 56%.

In the same period, the number of logical attacks increased by 86%. It is striking that the type of logical attacks favored by attackers is changing. The proportion of skimming attacks, where the data from credit or bank cards can be accessed by technical manipulation of the card reader on ATMs, is falling – in Switzerland, thanks to the geo-blocking technology introduced by SIX, in particular. In contrast, the number of black box attacks is increasing dramatically – not just in Switzerland but internationally. With this attack pattern, a small computer is installed in the ATM via which malware can be installed or logical attacks carried out. The European Association for Secure Transactions (EAST) reported an increase in black box attacks of 269% for Europe in the first half of 2020.

Another attack vector is also playing an ever greater role: cyber attacks on ATM networks, where hackers obtain access to banks’ IT networks and carry out the attacks from there.

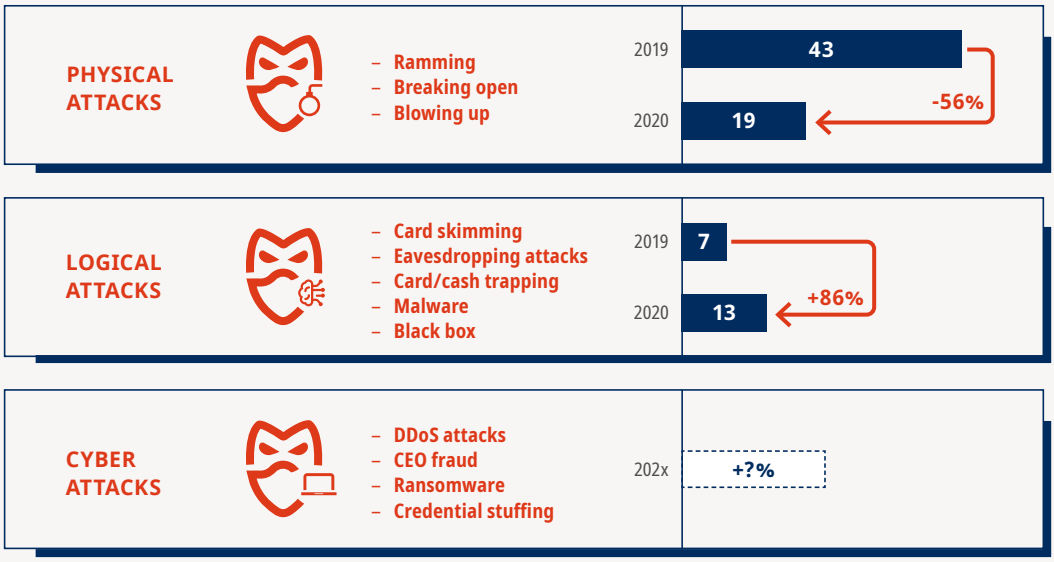

Fig. Changed attack patterns on ATMs in Switzerland, source: SIX

Challenge: Cyber Security

Cyber security is a global challenge. This is reflected not least in the global wave of cyber attacks that has been running against government departments, telecommunication and commodity companies since March 2020 and in the course of which hackers penetrated the US Department of Commerce and the US Department of the Treasury in December 2020. No sector is subject to as many attacks as the financial sector. "Cyber crime groups try to take financial institutions hostage and commandeer digital transformation efforts," states the Cloud Provider VMware Carbon Black in its security report "Modern Bank Heists 2020". Accordingly, the number of cyber attacks on financial institutions increased by 238% in the first quarter of 2020.

At first glance, it may be reassuring that the Cyber Security Report 2020 published by SIX still shows a very small number of cyber attacks for Switzerland compared with other countries. However, the fact that reports of cyber attacks to the Reporting and Analysis Center for Information Assurance (MELANI), which is affiliated to the National Cyber Security Center (NCSC), are (still) voluntary must be taken into consideration here.

The fact is that cyber attacks on banking systems are a growing threat. Increasingly, this also applies to ATMs.

Future Threat Level for ATMs

Hackers are still concentrating on DDoS attacks, where capacity to process inquiries is exceeded in a targeted attack, meaning that a target system is disabled. Scams such as CEO fraud attacks, credential stuffing – systematic misuse of access data – and ransomware are also used, where malicious software refuses access to data through encryption. It is a question of time when hackers will use their access to banking networks not merely to encrypt data and steal data but also to launch large-scale attacks on ATM networks via this route. They could use their malware to trigger cash payments, which they then collect from ATMs. If they succeed in doing this, the method will spread round the globe extremely quickly. Hackers join forces internationally and exchange expertise and data to develop more effective methods of attack jointly.

Swiss financial institutions must confront the threat of logical and cyber attacks. Concentrated, efficient and effective action by all ATM stakeholders is required to set up an early warning system and develop coordinated defense measures.

Security Threat of Swiss ATMs

The current threat situation facing ATM security requires orchestrated action by all ATM stakeholders. All operators of ATM infrastructure are faced with the same risks and threats. But there is no holistic view of all attacks. In dozens of cases, work is being carried out simultaneously on solutions. Instead of pooling their resources, several financial institutions are monitoring the same sources in parallel. Currently, continuous learning about the type and manner of attacks is taking place only individually at the level of the individual financial institutions. The decline in the significance of cash and consequently of ATMs also means that valuable ATM knowledge is being lost as posts are not being filled.

Ultimately, there is no centrally managed communication between ATM stakeholders. There is also a lack of infrastructure through which waves of attacks and their methods can be promptly recognized in their entirety and forward-looking warnings issued in good time or effective countermeasures taken.

Made in Switzerland: The New ATM Security Service

Swiss financial institutions together with SIX focused on current and future threat trends as early as 2018. Cross-bank workshops were initiated, security incidents and attacks analyzed. There is a consensus that a new central ATM security service is needed to

- get a holistic perspective of attacks
- recognize risks specifically and initiate suitable measures
- provide high quality reports
- provide a central platform for standardized data and information
- establish a central point of contact for all Swiss financial institutions
- develop an institutionalized alarming and information chain

On this basis, SIX has started to develop ATM Security Services. As part of the new range of services, ATM events, messages and alarms from the participating financial institutions will be monitored centrally, information from MELANI, EAST and other public sources about new threats relating to ATMs will be evaluated and warnings from ATM manufacturers taken into account.

The Central ATM Security Framework Provided by SIX Is Being Expanded and Will Be Based on Three Pillars:

THREAT INTELLIGENCE & SECURITY ADVISORY

Central monitoring of global news of new approaches and threats to ATMs as well as regular information to participating financial institutions

SECURITY & EVENT ANALYSIS

Central analysis of potential risks to ATMs in Switzerland

ALARMING & RAPID RESPONSE

Event-driven alarming and continuous information as well as provision of recommended action for participating financial institutions

LEARN MORE

SIX BBS Ltd
Hardturmstrasse 201
P.O. Box
8021 Zurich
T +41 58 399 4012
cash@six-group.com