DIEBOLD NIXDORF PERSPECTIVE

Five ways your ATM's logical defences could be stronger

Joerg Reuter
Diebold Nixdorf

By Joerg Reuter, Business Development Lead, Security, and Bernd Redecker, Director of Corporate Security and Fraud Management, Diebold Nixdorf

When the WannaCry ransomware attacks occurred earlier this year, we were inundated with questions. Although banks were not the main target in this particular instance, the media publicity made stakeholders in every industry understandably jittery, and with good reason – Symantec reported that ransomware attacks increased by more than 36% from 2015 to 2016, with 463,841 infections detected in a single year.[1]

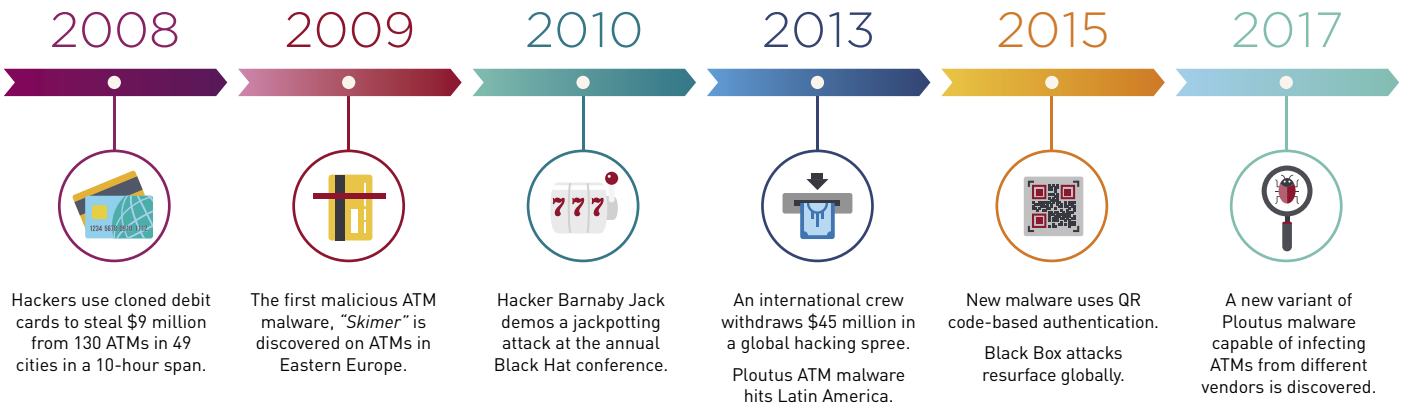
Increasingly, the question is not *if* your organisation will be attacked, but *when*. What is most troubling is that it is very difficult to predict how your organisation will be threatened, which means you must be prepared to fight on every front. Physical attacks still happen around the globe, from explosions to ram raids. Skimming is on the rise in certain regions even as it decreases in others. Meanwhile, newer threats such as logical and hacking attacks are becoming more complex and subtle. Over the past few years, logical attacks have become a major challenge and one that is only getting bigger (see figure below).

Security must be a top priority – with the right partner, tools and strategy, holistically protecting your network is possible. We are advocates of a strategic, multi-layered approach that serves two functions: one, it provides back-up protection in the case of an attack, and two, it ensures that your network is protected no matter what form the attack takes. While every organisation's needs are different, there are a few basic guidelines that can help ensure your data and systems remain secure.

1. Evaluate your IT security team's approach to ATM security

A traditional IT department at a financial institution (FI) may be tempted to treat the ATM channel as if it's just a group of oversized PCs. Perhaps up to 80% of the policies and security tactics are comparable, but the other 20% can present a huge problem. The ATM is an unattended terminal running 24/7, often 'out in the wild'. Its requirements are dramatically different from that of PCs. This means that the security guidelines which were created for your office PCs are not 1:1 applicable to ATMs. Your ATMs can – and should – be talking to only two or three dedicated systems and nothing else. There is no need for them to talk to an arbitrary web or file server. An ATM network should be almost entirely locked down and

HACKING METHODS CONTINUE TO EVOLVE & REFINE



restricted to the crucial connections. An attack like WannaCry can usually be thwarted at an early stage with this type of highly protected network.

2. Lock down your ATM

In a similar way, the software running on an ATM is well-defined and only has a limited number of predetermined tasks to fulfil. There is the consumer-facing application that also talks to the authorisation systems, some operational tools – and that's it. This means that every other functionality can be blocked, effectively locking down the ATM and reducing the attack surface considerably.

Our Terminal Security Suite has been developed to meet these specific demands. It is designed to operate in a self-service environment, with integrated tools that ensure the same look and feel, the same interface, the same run time, and blanket protection across an entire network. And because we developed it in-house, FIs can feel confident that the maintenance and updates ensure protection against the latest security threats.

3. Be prepared for new types of attacks

In our digitally driven world, FIs are providing new consumer touchpoints and banking services. As trends like mobile cash, cardless cash withdrawal via NFC, contactless transactions, IoT-enabled interactions and the like continue to proliferate, they're opening the door for new security concerns. As attacks become more diverse, your countermeasures must become not only more holistic, but more creative. The ability to be flexible and think 'outside the box' will be critical – but it will also be vitally important to stay on top of the latest logical attacks. At Diebold Nixdorf, we work hard to make sure these innovations maintain or even improve security for consumers and FIs.

4. Talk to other 'good guys'

The bad guys are out there sharing their knowledge. They sell hacking tips, methods, even software that's ready to download and use 'right out of the box'. They work in global, interconnected teams. And they're continuously evolving.

We must be just as informed as they are, and that means sharing knowledge and awareness. Our Corporate Security & Fraud Management team is a global community of Diebold Nixdorf security experts, from service technicians to field engineers to software designers, dedicated to sharing our expertise and learnings with our customers. This unique strength means we're able to counteract threats more quickly and operate in a more proactive manner.

5. Consolidate and simplify

Fraudsters have never been more sophisticated. They're learning not just how to exploit ATMs via bombs, skimmers and hacking methods, but through a deep knowledge of internal processes and company culture. They take advantage of loopholes and weaknesses that they've discovered by closely researching individual organisations. Attacks are becoming more complex, and making sure the self-service fleet is protected end-to-end against all kinds of attacks requires a lot of time, resources and knowledge. Simplifying and consolidating your approach not only makes your security stronger, it frees up resources that can be devoted to other areas of your organisation.

If you want to relieve your teams of the burden of keeping on top of self-service security, you can rely on Diebold Nixdorf's Managed Security and Compliance Services. Our end-to-end fleet services meet ever-evolving ATM security requirements and ensure compliance to relevant regulations such as PCI DSS. ■

Find out more about how you can implement a multi-layered approach to security at DieboldNixdorf.com/security

[1] *Internet Security Threat Report*, Symantec, April 2017

Bernd Redecker
Diebold Nixdorf

Fraudsters are learning not just how to exploit ATMs via bombs, skimmers and hacking methods, but through a deep knowledge of internal processes and company culture

DIEBOLD NIXDORF