DIEBOLD PERSPECTIVE

Multilayered security protects identities and combats malware

Mitigating the big three self-service channel threats

Nicholas Billett
Diebold

By Nicholas Billett, Senior Director, Core Software & ATM Security, Diebold

Fraud. Logical attacks. Physical attacks. These are the 'big three' threats financial institutions and consumers face at the self-service channel. Conquering the primary threats to security and staying ahead of would-be criminals requires vigilance – and multiple layers of protection.

A multilayered security approach is designed to pinpoint every attack vector in realtime to effectively secure self-service networks. By using a strategy that integrates hardware, software and services, financial institutions can be assured of having the most comprehensive and reliable protection. Every layer serves to defy hackers, prevent intrusion and help stop crime before it happens.

A multilayered approach is designed to pinpoint every attack vector in realtime

Protecting against fraud

Mitigating fraud begins with shoring up defences on the consumer-facing side of the channel. At self-service terminals such as ATMs, criminals may attempt to install skimming devices, fake PIN pad overlays or mini cameras to capture card and PIN information. Alternatively, they may install card or cash trapping devices, which prevent consumers from being able to retrieve their cards or cash withdrawals. At the computer workstation or mobile device, criminals may install malware or keyloggers, or pursue other attack vectors.

Combating skimming and trapping starts at the card reader, where advanced technologies can deter fraud attempts, detect foreign devices and prevent criminals from obtaining data, cards or cash. Advanced readers use a variety of methods to prevent successful skimming, including uniquely shaped fascias, jitter mechanisms that vary the speed of inserted cards, and gate-locking mechanisms that ensure the card reader gate remains completely closed when not in use.

Motion and alarm sensors can detect the presence of a skimmer or trapping device and alert financial institutions and monitoring providers. Such sensors continuously monitor the card reader environment and lock down terminals when a foreign object is detected. Furthermore, readers can prevent the removal of trapped cards, and terminals can report anomalous activity.

To provide all this and more, Diebold has developed the ActivEdge™ card reader that prevents all known forms of skimming by shifting card insertion 90 degrees to the long edge instead of the traditional short edge. The reader uses encrypted technology to provide advanced layers of protection to combat card skimming, trapping and fishing attempts, and it inhibits criminal modifications to the card reader and prevents fraudulent data capture. Moreover, its automatic gate-locking functionality prevents fraudsters from freeing trapped cards.

Beyond securing the card reader, there are additional layers of fraud protection that financial institutions must consider for the self-service channel. These include solutions that mitigate shoulder surfing, PIN interception, false transaction reversal, dispenser false fronts, secure mobile and online banking sessions, real time exception monitoring, software stack management and more.

Combating logical attacks

A multilayered security approach protects consumers – before they even insert a card into an ATM or start an online session – by locking down systems against logical attacks, which seek to compromise data and applications. Securing the self-service channel requires constant evolution to counter these increasingly sophisticated attacks and overcome user errors.

Financial institutions can pile on layers of protection to withstand a wide variety of logical attack vectors. For example, to counter criminals' attempts to pilfer stored data by removing ATM hard drives, deployers can install encrypted hard drives, which make data inaccessible when the drive is removed from the ATM PC. They can implement solutions that encrypt and lock a hard drive if the ATM boots from an alternate source (such as an external CD/DVD, USB or external hard drive). There are also solutions that halt an ATM PC's boot process if the terminal detects an unauthorised change to its Basic Input-Output System (BIOS). Another example is to sandbox online banking sessions and implement heuristic capabilities to understand and risk-rate safe and unsafe behaviours at the channel.

Newer malware threats such as Ploutus and Tyupkin, which trick ATMs into dispensing bills by entering a keypad sequence or sending a text, require access to a terminal's interior. To thwart such attacks, operators can use existing physical security sensors in the ATM to detect unauthorised access to the computer. Furthermore, financial institutions can leverage outsourcing partners to manage software updates and information security controls to prevent malware from being added to the ATM.

But regardless of the self-service channel, a key aspect of a successful solution is realtime protection and proactive *remote* intervention. Rather than send technicians to visit each terminal to update software or to correct an issue, financial institutions can streamline operations using realtime remote ATM channel management solutions. And instead of trusting that a consumer's laptop is running up-to-date patches and is malware free, their sessions can be sandboxed for everyone's protection. By leveraging remote connectivity, financial institutions can reduce expenses, respond more quickly and provide a safer environment for consumers.

Mitigating physical attacks

To defend against physical attacks on the ATM, it is critical for a financial institution to know the moment a breach attempt has occurred so that it can take immediate corrective actions. The corollary is to know how to respond appropriately when an attack is underway. That is why realtime monitoring and preplanning is so important. Integrating advanced sensors and alarms and having worldwide visibility into new attack vectors can help institutions promptly detect and thwart attacks.

Coupling those alerts with remote monitoring provides another layer of defence that enables remote investigations and immediate corrective actions, including remotely shutting down any session that is used to launch an attack.

Advanced safes, locks and anchoring systems provide additional layers of physical protection where applicable. Tie all of these efforts together with a solid response plan, and you have created an ecosystem that minimises residual risk for banks and consumers.

Layering up

Security is critical to maintaining consumer confidence in the self-service channel, which in turn is key to preserving a financial institution's brand. By adopting a multilayered, process-driven, realtime security approach, financial institutions can more effectively monitor, identify and mitigate potential risks 24/7. Only by deploying layer upon layer of security measures can an institution sufficiently offer reasonable protection against fraud, logical attacks and physical attacks, assuring a secure environment for consumers. ■

To learn more about how a multilayered security approach can protect your network, customers, assets and brand, visit www.diebold.com.

Deployers can install encrypted hard drives, which make data inaccessible when the drive is removed from the ATM