bizcommunity

Understanding cyber-criminals is key to prevent attacks

Understanding how cyber-criminals operate and the techniques they use is key to preventing attacks. But how do we do that when cyber-crime evolves seemingly by the minute and new threats emerge daily?

By William Lawrence 11 Sep 2014

Cyber-criminals are smart and well-connected. They do a few things particularly well that ensure their success - and banks should take note.

Most criminal syndicate members have never met face to face. They communicate over social media, blo and the Deep Web, gathering information about their victims - names, ID numbers, credit card details - to provide to other criminals. They share resources and develop sophisticated technology, which they sell to other syndicates.

Current fraud detection systems are no longer fit for purpose. Banks use disparate systems that focus on single lines of business or channels, rather than adopting a holistic view of the customer. Typically, banks have one solution for fraud detection in current and savings accounts, another for credit cards and yet another for home loans.

Predictive models

These systems act on a transactional and single customer level using predictive or reactionary models but the biggest problem is that these systems don't talk to each other and the different departments don't share information. Information and knowledge is one of the best defences a bank can deploy to protect its customers and itself from fraud.

Between 70 and 100 new phising malware websites appeared each day during the World Cup. Phishing occurs when fraudsters send emails supposedly from reputable organisations, such a banks, that try to get recipients to disclose personal information, such as their credit card or Internet banking details.

When those tactics stop working, they simply deploy new ones and replicate others that have worked in the past.

While banks evolve in the sense that they're always introducing new products and services, in many cases these are monitored in isolation by disparate fraud detection systems. Current solutions don't keep pace with advances in cyber-crime, to the detriment of the organisation and

its clients.

Hybrid analytics

The challenge for banks is to balance the customer experience by putting measures in place to prevent fraud. The best way they can achieve this is by adopting advanced, hybrid analytics, which provide an end-to-end view of the customer.

Fraudsters send emails or set up websites that automatically install malware on a user's computer. Some Trojans allow cyber-criminals to discreetly change transaction details, log key strokes and grab information and are even able to do a measure of analytics to record online behaviour, such as what time of day you typically log onto your Internet banking profile and wha transactions you make.

Criminals often engage insiders to understand banks' fraud detection environments, such as wl business rules or thresholds they apply, and circumvent these. For example, a bank may only scrutinise transactions over R10,000 for fraudulent activity. Fraudsters will then only initiate transactions at, say, R9,000 to avoid detection.

Banks need to adopt equally sophisticated technology and smarts to ensure fraudulent transactions are identified and blocked before the money leaves the account in question.

Online banking sessions

Advanced solutions cover multiple points of vulnerability and use 'event stream processing' to analyse online banking sessions at a transaction level, customer level and network level. Using normal business rules, anomaly detection techniques and advanced analytics, these solutions v raise flags, in real time, if someone enters their login details incorrectly multiple times, if they access their accounts from an unusual device or location, if they add a beneficiary who is on a watchlist, such as a suspected mule account, if they make multiple payments to new beneficiarie and if they display unusual 'session' behaviour, such as if they log in using the 'Shift' key on the left when they usually use the one on the right of the keyboard - an activity fraudsters are unlike to know.

In isolation, these incidents would not necessarily trigger a warning, but if multiple flags are raised, the transaction may be blocked immediately, depending on its overall fraud score, and w be escalated for further investigation.

By sharing information between departments and systems and by harnessing analytics technology that is able to analyse transactions and user behaviour in real time, banks will be in a better position to fend off cyber-attacks and better protect clients.

ABOUT THE AUTHOR

William Lawrence is Regional Practice Lead: Fraud and Financial Crimes at SAS.