FinTech Threat: The Malicious Insider

Whether motivated by personal financial gain, revenge, dissatisfaction, or the desire for respect, one of the biggest threats to your organization is sitting right underneath your nose. Out of the whopping 41,686 security incidents and 2,013 data breaches profiled in the 2019 Verizon Data Breach Investigations Report, **34% involved internal actors** (Verizon LLC, 2019). The individuals tasked with protecting your enterprise are a great asset but also pose a tremendous threat.

The likelihood of an insider threat increases for organizations that store sensitive customer data, have valuable intellectual property, or support critical infrastructure. Although multiple industries meet these criteria, history has proven that Financial Services is often a target with devastating results. We have seen prized assets catalogued, exfiltrated, and sold to the highest bidder.

Whether that data provides customer banking details to initiate transfers, contains proprietary trading models, logs anti-money laundering audit trails, stores wealth management client information, or provides support to another key function, the reality is that data must be stored and made accessible for the organization to operate. However, as these organizations continue to harden their evolving network perimeters to focus on keeping the external threat actors out, they overlook the people who already have unrestricted access to their network.

Simply put, an insider threat is a security risk to the organization that comes from within the business itself. Common threat actors include current and former employees as well as contractors, contributors in the supply chain, or really anyone that has or had access to the business in some way or another. Before, we dive deeper into the types of insider threats, it's important to realize that the attack originates from within and doesn't have to be intentional. This is why the insider threat is one of the most complicated and costliest to detect of all types of attack.

At this point, it might be useful to examples showcasing the different types of insider threats. For this, we will use threat actors as defined by the Verizon report (Verizon LLC, 2019) . While reviewing the different actors, think to yourself if any sound familiar…

- **The Careless Worker**: Misuser of assets
  - Installs unauthorized applications
  - Has unapproved workarounds
- **The Inside Agent:** Stealing information for outsiders
  - Recent behavioral changes
  - Does not follow company policies
- **The Disgruntled Employee:** Destroying property
  - Was glanced over for a promotion
  - Demonstrates change in approachability
- **The Malicious Insider:** Stealing information for personal gain
  - Unusual working hours
  - Increased access requests
- **The Feckless Third Party:** Compromising security
  - Negligent use of company assets

Organizations have been focusing more on ways to mitigate insider threats, but this is impossible to do without a clear understanding of what data is valuable, where it is stored, and who is accessing it. This is common practice for security teams who routinely perform threat modeling in the early stages of any engagement. Organizations can benefit greatly from bringing in an external organization that does this routinely.

Back to Financial Services and FinTech organizations who are a prime target because of the importance and allure of the assets in their control. These threats can pose huge losses organizations with **the average cost of an insider threat being $8.7 million in 2018**[1]. When faced with a problem, the solution has been to create programs that integrate user activity monitoring, data loss prevention, security and event management, analytics, and digital forensics with mixed results.

The insider threat problem is complex and requires a bespoke solution for your organization. Leveraging off the shelf tools create gaps. Insiders have a familiarity and access to sensitive data which will make detection more difficult. It's important that you know where those shortcomings exist and to get routine practice.

Publicly available tools are also adding sophistication to every step of the insider threat kill-chain; furthering headaches for insider threat programs. Education about these attacks is crucial and we have created a repository showcasing some of the cunning processes threat actors are using for the usual last step of an insider threat campaign, data exfiltration. Our goal with this curated list is to raise awareness about the specific ways and tools threat actors are exfiltrating data from target organizations.

Whether using the sound produced from a CDROM drive, the Spotify API, or cloaking one form of data in another, sensitive data is leaving organizations under the radar of common detection tools. These novel techniques are ever changing and widely available. But before we scare you with all the possibilities, there a few ways that you can immediately reduce the risk for your organization.

Three tips to immediately reduce risk

1. **Encrypt sensitive data**: Whether stored or travelling across a network, it's important to encrypt sensitive data. If a threat actor does intercept network traffic, steals a hard drive, or accesses a data store, they won't be able to immediately read or make meaning of the data.
2. **Know your risk exposure:** Threat modelling is a great tool that can allow your organization to maintain an accurate risk profile and can be used to help mitigate risk organization wide by aligning stakeholders, budgets, and strategies.
3. **Conduct routine assessments:** The overall security posture of an organization is in a constant state of flux. It's critical that components are routinely tested to validate if existing measures are working

Security Innovation has been reducing organizational risk for over a decade by providing software security services and trainings to FinTech and other clients with a reputation to protect. Curious to learn more about our security expertise in Financial Services and FinTech, checkout our blog post and accompanying Defcon talk discussing the OFX protocol and your *Bank's Digital Side Door*.

[1] https://securityintelligence.com/news/the-average-cost-of-an-insider-threat-hits-8-7-million/