Secure critical data in financial services

Manage cyber risk in face of increasing attacks

Financial institutions are a prime target for cybercriminals, because they control vast amounts of money and store huge volumes of personal customer data. With attacks becoming increasingly sophisticated, banks and insurance companies need to be informed to stay on top of these attacks.

Cyberattacks cost the financial services organizations more than any other industry, according to a report by the Ponemon Institute[1]. Worryingly the rate of breaches in the financial services industry has tripled over the past five years.

The biggest impact of cyber breaches on financial services organizations are primarily business disruption and information loss, which together account for 87 percent of the cost to respond to cybercrime incidents, with revenue loss accounting for only 13 percent[2].

Financial institutions invest heavily in a bid to keep their infrastructures safe, but with the rise of omnichannel communications, online banking and mobile apps, the threat vector has expanded. The notorious Carbanak Group, also known as the Cobalt Group and FIN7, continue to attack vulnerabilities in financial institutions. Most recently it has launched a spear-phishing email campaign containing malicious links. Since 2013 the cyber gang is believed to have stolen one billion euros from one hundred financial institutions in forty countries using malware.

Digitization has opened the doors to cybercrime

Technology has made it much easier for cybercriminals to carry out traditional crimes such as fraud, robbery and extortion, using digital techniques such as distributed denial of service (DDoS), ransomware, spear-phishing and malware amongst others.

Digital transformation, regulations supporting open banking APIs, the internet of things (IoT) and all-IP mobile networks, which allow mobile device users to move from one network to another while maintaining a permanent IP address, are all contributing to increasing the vulnerability of financial services. With a growing threat landscape comes the question of trust. Consumers trust financial institutions with their money and data, but this can quickly erode in the face of large-scale attacks.

80% rise in cyber attacks against financial services companies in the UK in 2017[3]

20% increase in spending on next generation authentication by retail banks in 2018[4]

40% increase in the average cost of a cybercrime in financial services in three years[5]

1 billion bot attacks involving 210 million fraud attempts in first quarter 2018[6]

orange™ Business Services

1, 2, 5 The Ponemon Institute: Cost of Cybercrime study 2018
3. Financial Conduct Authority 2018
4. IDC: top 10 worldwide financial services predictions
6. Threatmetrix Cybercrime Report Q1 2018

Navigating the regulatory jungle

The financial services industry has a complex regulatory jungle to navigate. This includes industry-specific regulations, such as the Dodd Frank Act and the Basel II accord, which govern how to protect organizational data. In addition, there are general regulations that also apply, including the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS), which aims to achieve a high common level of network and information systems security across Europe. And inevitably more will follow.

This complexity makes regulation compliance a major undertaking and one that has become costlier and more time consuming. It is a major concern for CIOs, who must be ready to shift in line with a changing legal environment. At the core of these regulations is the need to protect the confidentiality integrity and availability of a stakeholder's data. Alongside security officers, CIOs are responsible for securing this information and are ultimately accountable.

Investing in people is key. Putting time and resources into training and awareness courses across the organization on cybersecurity pays dividends. This reinforces everyone's role in the organization in keeping it as secure as possible.

Securing the customer's financial journey

Digitization in financial services requires end-to-end cybersecurity. Strategies include:

- Utilizing audits and consultancy to ensure a robust security strategy
- Instigating threat intelligence
- Deploying advance threat protection
- Enhancing overall cyber risk management
- Defending and monitoring critical assets

To find out more visit https://www.orange-business.com/en/solutions/security

7. Gartner Top Ten Security Predictions 2017

orange™ Business Services

Five steps to delivering a secure financial environment

1. Run a risk assessment to build your security strategy and regularly review it. Risk assessments can be run on any application, function or process. Create an operational framework that identifies the internal and external systems critical to your organization's operation and processes.

2. Ensure you detect known and unknown threats in real time. This provides immediate insight into threats and their associated risk to the organization. It allows you to make decisions fast on which vulnerabilities to tackle first.

3. Ensure that you can qualify, retain and remediate attacks. According to Gartner, 99 percent of vulnerabilities exploited will be already known by security professionals[7]. Automated vulnerability capabilities include changing workflows and rules, patching vulnerable software and networking devices and changing configurations.

4. Use advanced analytics and artificial intelligence (AI) to proactively monitor and investigate emerging threats, fraud and data leaks. It can detect patterns in human behavior and when it thinks something is amiss, it will alert you.

5. Keep your threat intelligence up-to-date. Threat intelligence provides context, indicators, heightened awareness, and actionable responses on current or emerging threats. Continuously tracking evolving cyber threat landscape is critical to preventing cyber attacks.

Why Orange?

- **1,200+ multi skilled experts worldwide**
- **9 SOCs, 4 CyberSOCs and 4 CERTs**
- **24/7/365 global services**
- **Proprietary threat intelligence database and real-time feeds**
- **Independent CERT and Epidemiology lab to qualify and remediate emerging threats**
- **720 multinational security customers**