Picture credit: Getty

FINANCIAL SECURITY BREACHES

Mike Smart *explores the best way to tackle potential breaches in the financial industry without affecting service and security*

Protecting valuable and sensitive financial data and maintaining customer trust through delivery of consistent, secure service is a key goal and priority for the finance industry. Any disruption to service carries potential negative reputational and financial consequences for an organisation, so care must be taken to maintain service, even during times of maintenance and upgrades. In the wake of high-profile outages from the likes of TSB bank and payments firm Visa, regulators are now demanding that IT managers and financial service providers improve their operational resilience or face penalties that are likely to result in further financial and reputational losses. However, any processes implemented must keep usability in mind, to avoid excessive downtime and adoption of workaround software by employees, which compounds issues surrounding security by introducing unauthorised applications into the organisation's environment.

An outage can have serious continued repercussions for a company. Even though the TSB outage occurred in the first half of 2018, the dust has yet to settle and the effects are still being felt. In that case, the outage was caused by problems which arose during migration of data, but it's easy to see that an outage due to a cyber attack, system outage, or data breach is likely to have even more negative consequences. The financial cost of a data breach is likely to be significant under GDPR and the reputational impact will continue to be felt in terms of loss of customer trust. In June 2018, the Bank of England announced that it will demand new minimum standards of service that it expects financial companies to deliver in the wake of a cyber attack or major IT failure. This aims to prevent extended periods of disruption to customers and minimise the resulting economic impact.

OPEN ALL HOURS

The start of 2018 marked the launch of new Open Banking standards in the UK, in order to align with the European regulation of the Revised Payment Service Directive (PSD2). Under Open Banking standards, the UK's top nine banks must open their APIs to third parties, to allow the flow of financial information to third parties, with the customer's consent. The aim is to improve competition between the providers of financial services, as well as allow new players to enter the space in order to provide the customer with the best deal. This has forced traditional banks to rethink their internal IT infrastructure, as well as their methods for fraud detection and prevention. A major element of this change is maintaining visibility over the vast amount of data flowing out of the organisation via these new open APIs, coupled with a deep understanding of the activities occurring within the internal environment.

In order to maintain high performance and accessibility – even during times of service interruption due to incidents (such as data breaches or system failures) or routine security updates – while protecting sensitive content, the network must have high resilience, including availability and continuity. Organisations must be able to provide consistent service through a system, allowing for updates to be performed when they are needed rather than waiting for scheduled windows of time without disruption. From an end-user's perspective, a smooth experience with no interruptions has to be achieved across the whole network, ensuring consistent reliability.

Like TSB, Visa faced financial penalties for failure to protect its customers

> **MAINTAINING SECURE SCALABLE CONNECTIVITY BETWEEN DIFFERENT SITES MUST BE A PRIORITY**

Widespread service disruption can have devastating consequences for an industry based on trust. Unhappy customers will not hesitate to voice their displeasure on social media platforms and additionally companies remain answerable to various regulatory bodies, including the Financial Conduct Authority (FCA).

This need for high availability must be balanced with the primary role of the network security: protecting vital assets. Securing the network begins with correct configuration and must be implemented at the start. In the end, systems and technologies will not be robust if setup is incorrectly configured and contains critical security holes which have not been addressed. Misconfiguration is, in fact, the result of human error, which is the leading factor in security failures. As much as 80 percent of unplanned outages are due to changes made by administrators or developers who have not carefully considered potential pitfalls in their plans. Financial institutions simply cannot afford this downtime.

On top of security concerns, fixing issues requires increased resource investment, which negatively affects profitability and exacerbates the time that the service is offline. Misconfiguration also leads to increasing network complexity and makes overall control and troubleshooting more challenging.

Network management systems play a critical role in avoiding human error and optimising time and resources used in network operations. All of this has a direct impact on the perceived security level and recurring costs. Understanding the activities taking place within an organisation's environment is fundamental and visibility is a key component of this. In this age of digital transformation, the more distributed and virtualised the network gets, the more essential remote management capabilities become. Ensuring visibility across a network starts with a Next-Generation Firewall (NGFW) central management system. These management tools must enable organisations to rapidly react to network and business changes and provide constant control and visibility over the network.

CHANGING DEMANDS

At the same time, these tools must act in a way that does not hinder internal processes or negatively affect the user experience. This would result in increased IT security workarounds being implemented, which would compound problems surrounding visibility. If a financial organisation is not keeping up with the changing demands of their workforce, employees will try to find workarounds or use personal technology that allows them to complete tasks effectively. Often these applications represent blind spots when it comes to network visibility and can leave organisations vulnerable.

As organisations increasingly move more and more of their infrastructure to the cloud, network security needs to evolve with it. Most organisations will be looking to extend network security to include not only the centralised infrastructure and data centres, but also into public cloud infrastructure and branches. Modern NGFW vendors are integrating networking capabilities like SD-WAN in a bid to help network administrators to regain visibility and control of their expanding network.

There are many side benefits to implementing SD-WAN technology, one of the biggest is the reduction of WAN costs as organisations move from legacy dedicated MPLS networks to much cheaper local broadband connections for their distributed sites. Users get better direct-to-cloud performance, and these sites remain protected by enterprise class network security without increasing the management (visibility and control) overhead.

Forcepoint worked with UK-based Sword Apak, whose web-based Wholesale Floorplanning System (WFS) offered functionality to major financial institutions worldwide. As part of the Sword Group,

Sword Apak had access to a global infrastructure with offices in over 20 countries, providing financial institutions with a local presence as well as flexible ASP and in-house delivery options to support their worldwide funding operations. For years, Sword Apak operated using strictly a proxy-based firewall. Moving to a deep-packet inspection firewall represented a completely different design as employed in the Next Generation Firewall products. Ideally, one single point of failure at a network node should not fail an entire system. However, the dated firewall systems would not support this kind of functionality. Sword Apak's strict, proxy-based firewall began to fail as it lacked the features necessary to support a growing infrastructure. Particularly, inbound and outbound traffic on the DNS server had grown so much, as the company expanded, that it was far beyond feasible to run the current firewall system.

> A SMOOTH EXPERIENCE WITH NO INTERRUPTIONS HAS TO BE ACHIEVED ACROSS THE NETWORK

Sword Apak customers, as well, noticed growing traffic putting their network at risk. Consequently, they demanded a new firewall system in order to safely move forward with the company. In order to stay compliant with its customers, Sword Apak ultimately recognised the project at hand – the dated firewall system lacked the resiliency to continue successfully. In an effort to resolve this, the company implemented Forcepoint Next Generation Firewall as a 'customer compliance project'. The overall customer satisfaction from the project stemmed multiple, additional Forcepoint NGFW projects and eventually led to Sword Apak migrating some of its services over to the Forcepoint NGFW solution full time. The desired resilient, load-balance, secure environment was attained to manage the increase in network traffic. This allowed Sword Apak to utilise multiple network links/nodes to flexibly increase bandwidth and provide automatic failover when individual nodes go down.

MAINTAINING A REPUTATION

Protecting the vast amount of sensitive and highly valuable data held by financial institutions is critical to maintaining trust and safeguarding reputation. This industry is under an increasing amount of pressure to remain robust, even though no software solution is fool proof and will fail from time to time. Through working with a trusted vendor, organisations can implement an NGFW solution that blocks malicious threats without affecting user experience, even when vital network maintenance is being carried out or during a security incident. In addition, many financial institutions occupy different sites and operate in public cloud environments, so maintaining secure and scalable connectivity between these sites must also be a priority. By implementing network security that meets all of these criteria, financial institutions will continue to provide a consistent service, which withstands system failures and changes to the threat landscape ●

Mike Smart is a Security Strategist supporting customers across EMEA at Forcepoint. An evangelist for information security evolution, Mike currently works with global system integrators and consulting firms to drive change from an exclusively threat-centric approach towards behaviour-centric programmes.

The Bank of England has high demands for financial companies in the event of a cyber attack or major IT failure

Picture credit: Getty