

Security Connected for Financial Services

by Brian Contos, Global Security Strategy and Risk Management, McAfee, Inc.

The financial services industry encompasses a wide range of business models, including commercial and private banking, investment services such as asset and hedge fund management, stock brokerages, conglomerates, and many others. Because the nature of the business is highly sensitive and personal, financial institutions are heavily regulated with national and international mandates such as SOX, PCI DSS, GLBA, the Red Flags Rule, and European Union directives. To protect sensitive information and achieve compliance, financial services organizations have been early adopters of security controls that have helped mitigate threats originating from external and internal attackers for well over a decade.



According to a recent survey by the Anti-Phishing Working Group, financial services companies are the most frequent targets of online attacks that put sensitive personal information at risk.¹

Attacks against web applications constitute more than 60 percent of the total attack attempts observed on the Internet, according to the SANS Top Cyber Security Risks of 2009.²

Trends

New challenges and trends have emerged during the last few years. From the mortgage collapse to diminishing customer loyalty, issues faced by financial services organizations are leading to a search for ways to achieve greater profitability while better serving their customers. In general terms, profitability requires investments in marketing, operational efficiencies, and risk management. Web portals for business process outsourcing (BPO) and customer self-service (CSS) are key vehicles for this. In addition to BPO and CSS, agent portals, call center applications, and straight-through processing are emerging as web portal applications using legacy, customized, and commercial off-the-shelf solutions from SAP, Oracle, and others—as well as the specialized applications that run on top of these commercial solutions. Making use of these portals requires a high level of automation and a technically sophisticated back office with great dependencies on applications and databases.

The result is highly sensitive data that is easily accessible and has dependencies on complex infrastructure and partner networks. At the core are mission-critical applications for transaction processing built on top of databases that store the “crown jewels”—confidential business data. Risk starts to increase because traditional controls myopically focused on network security are unable to mitigate the data-centric attacks that target these applications and databases. The result is that organizations may have made major investments

in web portals but likely have not implemented the necessary controls to protect them. New business initiatives and the technology they leverage have outpaced security.

The Boiling Frog Syndrome

As the story goes, if you throw a frog into a pot of boiling water, it will jump out. However, if you place a frog in water that is at room temperature and increase the heat slowly, it will not notice and end up getting cooked. This is analogous to protecting web portals with nothing but network security controls. We’ve been protecting our IT environments for so long with network security controls that we think, or possibly hope, that they will protect us from next-generation threats that are, in fact, primarily focused on applications and databases (that is, sensitive data). Not only are controls designed specifically to protect data—a good idea from a security perspective—but they are absolutely essential when it comes to addressing sections of most regulatory mandates.

There is no question that within the financial services industry, web portals are considered mission-critical assets. To protect these assets, a combination of network security controls to protect systems, such as web servers and databases are needed, as well as data security controls to protect the information they process and store.

It is, however, more effective to approach this combination with a unified construct that allows network security and data security to complement

A recent example of insiders with legitimate trust and access taking advantage of their ability to capture sensitive data are the WikiLeaks incidents of December 2010, where sensitive government and military documents were posted for public viewing. In addition to the government, commercial organizations, including financial institutions, were impacted, as evidenced by "hactivist" distributed denial-of-service (DDoS) attacks that limited the availability of web portals.³

Web application vulnerabilities, such as SQL injection and cross-site scripting flaws in open-source as well as custom-built applications, account for more than 80 percent of the vulnerabilities discovered, according to the SANS Top 10 Security Risks 2009.⁴

each other rather than operate in disparate silos. Because this information is accessible by external users such as customers and partners, as well as internal users, to include privileged users such as system administrators and database administrators, it is necessary to consider threats from external attackers and insiders when deploying the controls.

Network security controls, such as firewalls and IPS, are absolutely necessary and provide protection for network-centric attacks. However, they are less effective when addressing attacks directed at application and database vulnerabilities. Here are just a few examples where data security controls provide protection beyond that of their network counterparts; note that the Open Web Application Security Project (OWASP) and Dark Reading have identified many of these in their Top 10 Most Common Vulnerabilities lists:

- Monitoring users (especially insiders) as they interact with data
- Monitoring how data is being moved around the network and endpoints
- Capturing sufficient audit information
- Encrypting data at rest and in motion
- Identifying application-level vulnerabilities
- Protecting against attacks such as:
 - » SQL injection
 - » Cross-site scripting (XSS)
 - » Cross-site request forgery (CSRF)

The McAfee Approach

What's the answer? The Security Connected framework from McAfee. This framework brings together the extensive portfolio of McAfee network and data security products and services with partnerships and an open architecture that maximizes flexibility and extensibility for a wide range of security controls.

When the Security Connected architectural framework is leveraged, situational awareness heightens, as blind spots left by one control are filled in by another, thus elevating the overall security posture of the organization. Organizations are able to make more informed decisions more rapidly because they have empirical evidence of nefarious activity across data and networks.

Protection from Internal Attacks

McAfee provides encryption solutions for data at rest and data in motion to help reduce the risk of a compromise revealing sensitive information.

However, encryption is only one aspect of data security. McAfee also offers data loss prevention on networks and endpoints to monitor what data is being manipulated, how, and by whom. Complementing these capabilities is database activity monitoring, which sees to it that robust audit reporting is captured on the database, ensuring that the audit information is intact even if it has been targeted by a privileged user such as a database administrator. When users interact with an application, the application in turn interacts with the database; this activity needs to be audited for analysis. If a database administrator interacts directly with the database, this activity is equally important for the audit process.

For fixed-function systems, such as ATMs and many specialized applications, configuration management plus dynamic whitelisting (lists of processes that are specifically approved to run) can also be used instead of or in addition to traditional signature matching through blacklisting (lists of processes that shouldn't be run). This helps protect these systems from malware as well as careless or intentional out-of-policy configurations. Typically, these mission-critical assets will also have network firewalls and intrusion prevention systems (IPS) in place guarding them.

All of these controls are necessary when protecting the back-end of the web portal from internal attacks.

A unified approach of conducting analysis through a centralized interface helps analysts gain more detailed security analytics, expanded reporting, accurate alerting, and streamlined management. This is particularly useful in financial services because IT staffs tend to be larger and more specialized and the architectures tend to be more complex with a greater dependency on availability and expedient transaction processing than in other business verticals. No individual or group typically understands all the interdependencies, so having centralized control for security analysis across networks and data increases operational efficiencies.

Definitions from the OWASP Top 10 Security Risks for 2010⁵

- Injection flaws, such as SQL, operating systems (OS), and lightweight directory access protocol (LDAP) injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
- Cross-site scripting (XSS) flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser that can hijack user sessions, deface websites, or redirect the user to malicious sites.
- A cross-site request forgery (CSRF) attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Protection from External Attacks

McAfee helps identify assets and their vulnerabilities. This is an important but often overlooked step in protecting web portals. Once again, because of the size and complexity of the portal architecture for most financial services organizations, identification of the web portals and their supporting infrastructure such as databases can be challenging without automated tools.

Next, McAfee identifies network-centric vulnerabilities associated with common network assessments as well as application-centric vulnerabilities associated with more involved application-level assessments that can help identify some of the previously mentioned vulnerabilities, such as SQL Injection and XSS. Web application firewalls (WAFs) are also used to block application attacks and virtually patch discovered application vulnerabilities. WAFs running along with McAfee network firewall and IPS solutions fill in all of the gaps.

Because of the Security Connected framework from McAfee, all of these controls are pulled together centrally so that the network and data security controls are operationally aware of attacks in progress, vulnerabilities on the targets, and countermeasures that are in place that can mitigate those attacks. This level of full-circle awareness means that all of your controls are leveraged in unison to combat attacks on web portals. Because

of the size and level of specialization of IT staffs at most financial services organizations, the Security Connected architectural framework results in management efficiencies by providing a centralized management console for database administrators, application developers, network professionals, systems administrators, and security analysts to strategize, monitor daily activity, and conduct root cause analysis for issues spanning routers and firewalls to solutions running on Oracle, SAP, and other platform.

Conclusion

McAfee provides the controls needed to protect web portals from network-centric and data-centric attacks sourced from malicious insiders and outsiders. This unified approach for prevention, detection, and response is conducted through a centralized interface that helps analysts get the information they need more quickly and empirically. The result: financial services organizations can reap the value web portals provide without taking on additional risk.

1 <http://www.antiphishing.org>
 2 <http://www.sans.org/top-cyber-security-risks/>
 3 <http://en.wikipedia.org/wiki/WikiLeaks>
 4 <http://www.sans.org/top-cyber-security-risks/>
 5 http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project



Brian Contos, CISSP, is director of global security strategy and risk management at McAfee. He is a recognized security expert with more than 15 years of security engineering and management expertise. He is the author of several books, including *Enemy at the Water Cooler—Real-Life Stories of Insider Threats* and *Physical and Logical Security Convergence*. He has worked with government organizations and Forbes Global 2000 companies around the world and is a sought-after public speaker and writer for the industry and business press. He also helped build several successful security companies. Contos was formerly chief security strategist at Imperva, chief security officer at ArcSight, and director of engineering at Riptech. In addition, he has held security positions at AT&T Bell Laboratories in São Paulo Brazil, Tandem Computers, and the Defense Information Systems Agency (DISA). Brian is a Ponemon Institute Fellow and graduate of the University of Arizona.

