TechTarget

E-Guide

The Expert's How-to on Vulnerability Management

This expert guide explores the steps your business can take to develop a data breach incident response plan and prevent data loss incidents. Also discover the five common Web application vulnerabilities and how to prevent against them.

Contents

Developing an incident response plan of attack in the data age

Christina Torode, Editorial Director SearchCIO.com

If you need any more evidence that your company's data is under siege, consider the findings of the 2013 Data Protection & Breach Readiness Guide, recently released by the Online Trust Alliance. The annual guide solicited research and input from numerous organizations, including the Identity Theft Council, the Open Security Foundation, the U.S. Chamber of Commerce, the Federal Bureau of Investigation and the U.S. Secret Service. The Open Security Foundation reported 1,478 incidents worldwide, but based on feedback from the FBI and the Secret Service, this figure represents a mere 10% to 20% of actual reported breaches, according to Craig Spiezle, executive director, founder and president of The Online Trust Alliance (OTA).

In this Q&A, Spiezle touches on the steps small- and medium-sized businesses (SMBs) can take to develop a data breach incident response plan and prevent data loss incidents. He also talks about how SMBs can address data privacy game changers such as social media, and why data collection should be minimized, even in an era where data is becoming a new form of commerce.

Are you finding that SMBs do not have a data breach incident response plan?

Craig Spiezle: Upwards of 60% [of organizations of all sizes] do not have complete plans, or don't have any plans. And those plans -- whether you are a Fortune 500, Fortune 100 or an SMB -- are typically not up to date.

Contents

An effective data breach response plan is something you don't just do once and then put on the shelf. So much changes so quickly -- the philosophy behind data collection, the use of cloud service providers, and even your own business purposes for your data. If you're not reviewing this at least every six months, your plan is incomplete or out of date, and that is just as bad as not having a plan at all. Let's say that six months ago you retained a new email service provider, are storing data in the cloud through Amazon, and decided to include credit card data. If you have a breach and your plan doesn't reflect those changes in your business, you're going to be chasing the wrong problem. You are not going to know where your data is or the extent of what you have that has been compromised.

You need to have a mechanism so that any changes to your data usage, collection or processes circle back and are kept in a single document as part of your incident response plan.

Who should be in charge of that process to make sure that happens?

Speizle: There needs to be one owner. However, putting all the responsibility on IT isn't a successful approach. Marketing, the IT department and even HR and finance need to be involved in that. You need a management team with those groups involved that is led by one person within those groups. That group should meet on a quarterly basis or semi-annual basis to review the document and go through a check list. If you're in health care or heavily regulated, that response plan may also involve legal, but the point is, the plan needs to have this holistic approach.

What are some cost-effective ways for SMBs to develop a data breach prevention plan?

Spiezle: SMBs need to ask if the data they have been collecting is still needed for what their business model is today. If you can minimize the data

Contents

as much as possible, then it's less of an issue of protecting it. The second part is how do you help protect that data? The common things that are overlooked are where that data is flowing in your organization. Is it going back and forth within the organization? Is it going to vendors or contractors and, if so, how are you protecting and encrypting that data? The key is recognizing that you will have a data loss incident; you will have to take steps such as minimizing the amount of data you have; you should be encrypting that data; and [you] should have a good handle on who has access to that data.

What we see more often in small organizations are employees who have global access to servers and data stores. Data should be on separate servers with use access limited to people that need it to do their job. We find that [regardless of company size] user access is not revoked as an individual's role changes, and the more passwords you have out there, the more access points can be compromised. One of the key points of doing a quarterly [incident response plan] review is revalidating who in the organization has access to what and if they need that access. And, if you have external sources, know who still has logon credentials to a service provider, for example.

How can SMBs balance the need to minimize data with the push to collect more data to improve customer service or sell data as a new source of revenue?

A company last week suffered a breach. They had credit card information that went back 10 years and it wasn't encrypted. Credit cards typically have a two-year life, so why are you keeping data that old? It is a bit annoying for a customer when they want to renew their membership and they have to give their credit card information again because it isn't stored, so it is not as customer-centric, but it is more secure.

To balance customer service with security, why not collect partial birth date information? You know their birthday is in June. That's all you need to send them some kind of promotion, or send them a reminder. Marketing still gets the information they need, but the data footprint and risk is reduced.

Contents

What should SMBs consider when developing a data loss incident response plan given the increasing number of employees using cloud services they purchased on their own?

Spiezle: Recognize that free services are being fueled by the data that they can collect. As a small business you want to be nimble and use those services, but recognize that there are some inherent risks with that. I'm not just talking about protecting consumer information, but [also] proprietary business information, your business plans and strategies. A data loss incident could not only impact your customers, but your employees and business partners [as well]. For a small business, it's harder to build back those relationships and your brand once they are tarnished.

Social media is a useful tool for smaller businesses, but does it create new data privacy problems?

Spiezle: Despite employee policy, all too often you do find employees putting confidential company information out there. That's not the number one issue though; the problem is the common passwords that people use. If [hackers] find your password for Facebook, they are going to try to use your password on Twitter or any other social platforms, because they know that people reuse passwords.

People also put a lot of information [on social platforms] that exposes them to spear phishing and other exploits. If I know enough about you, I can create a persona and try to convince you to share information with me.

Younger workers are used to sharing information on social platforms and they are a growing percentage of employees and customers. Is this changing the nature of what is considered private?

Spiezle: There is a generational perspective to data sensitivity and privacy, but I can tell you my own kids, who are now in college, are looking at internships and recognizing that they need to change what they've been doing [on social forums]. It underscores that privacy and data security and protection need to be everyone's job at a company. Whether you are big or a small company, that risk could be embarrassment, financial liability or business loss, which all add up to costs. You're not immune as a small business. If it means that you have to take your website down and management has to spend a week working through the problem, it's clearly a significant interruption.

Is the rate at which data losses are occurring increasing and are they going unnoticed longer because so much data is being collected and shared on a variety of devices and services?

Spiezle: Last year we saw a 34% increase in the number of reported breaches. The majority of breaches, however, are not publically disclosed. According to the FBI and Secret Service, we are probably only seeing 10% to 20% of the actual breaches being reported.

As for time to discovery, it isn't instantaneous in many cases. Often it's six to 12 months later. That underscores the need for small businesses to maintain their data logs for at least a year. This is counterintuitive to what I said about data minimization, but in the case of their logs, you want to be able to go back and see if there are any patterns that are trying to compromise the servers, or network connections that were unauthorized.

Contents

Contents

Five common Web application vulnerabilities and mitigations

Brandan Blevins, Assistant Site Editor

SOURCE: Thinkstock

Every three years, the Open Web Application Security Project (OWASP) updates its list of the top 10 most critical Web application security flaws. This list changes little from one iteration to the next; the same issues crop up repeatedly because enterprises consistently fail to address common Web application security flaws. Exploitation methods against these flaws have become so rampant that the criminals who build automated exploit toolkit include these methods in their kits, enabling less sophisticated cybercriminals to seek out and exploit Web app vulnerabilities.”

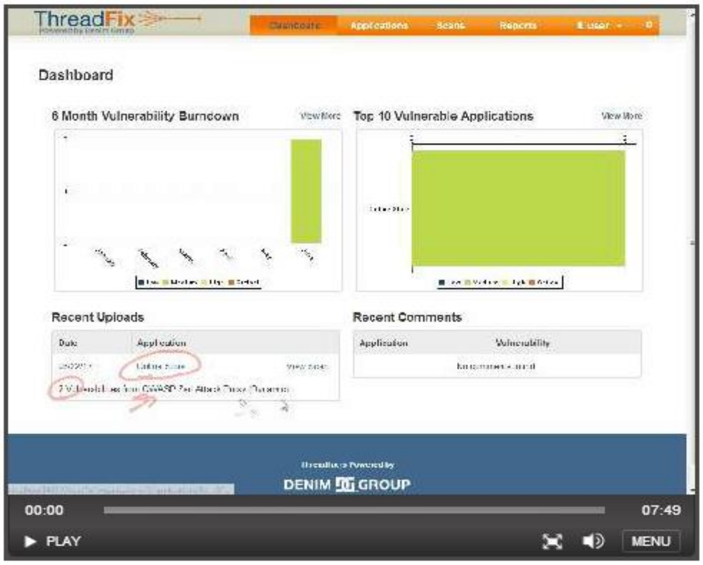
This Search Security slideshow, based on advice from application security expert Michael Cobb, explores five common Web application vulnerabilities from the OWASP top 10 list. He explains how each vulnerability surfaces in a Web application, how a criminal could potentially exploit it and provides mitigations for enterprises that have not yet remediated these Web app flaws.

To view the entire slideshow click here

Contents

How to use ThreadFix to simplify the vulnerability management process

Keith Barker



Click here to view the accompanying video

For any enterprise that develops several applications simultaneously, making security a focus during the development process can be a struggle. Scanning tools can analyze applications for vulnerabilities, but ranking the relative importance of each vulnerability and its fix status can be challenging: Exporting data from multiple scanners involving numerous applications in development can create confusion.

How can enterprises get a better handle on the vulnerability management process and ensure security issues aren't being overlooked? The open source security tool ThreadFix may just be the answer.

In this SearchSecurity screencast, Keith Barker, a Certified Information Systems Security Professional (CISSP) and trainer for CBT Nuggets LLC, presents a demonstration of ThreadFix, a vulnerability management tool offered by security consultancy Denim Group Ltd. With ThreadFix installed on one machine, Barker uses a client machine's browser to visit via proxy the BodgeIt store, a vulnerable Web application designed for penetration testing. Once the proxy captures the vulnerabilities from the BodgeIt store, Barker shows how simple it is to export the scanner data to ThreadFix. The tool is capable of aggregating export data from a variety of open source and commercial security scanners, including OWASP's Zed Attack Proxy and Nessus, which means most enterprises will have no problem using their scanner of choice. ThreadFix even accepts input from manual scans.

Barker then demonstrates how the exported scanner data can be sorted by team and by application, which helps simplify the enterprise vulnerability management process. If your organization is struggling to keep track of the security vulnerabilities discovered in a variety of applications, the free and open source ThreadFix tool can prioritize vulnerabilities and allocate precious infosec resources.

TechTarget

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

- SearchCloudSecurity
- SearchSecurity
- SearchFinancialSecurity
- SearchMidmarketSecurity