TECHNICAL BRIEF

5 Common eCommerce Security Mistakes You Can Avoid

Challenge

Keep eCommerce secure at a time when the threat landscape is dramatically growing and rapidly evolving.

At Stake

eCommerce sites must be flexible enough to support continuous change but secure enough to ensure customer transactions and data are safe and private.

Solution

Avoid these five common eCommerce security mistakes — and don't "go it alone." Work with security communities of interest, government agencies, and service providers to keep your online store secure.

Avoid these five common eCommerce security mistakes — and don't "go it alone." Work with security communities of interest, government agencies, and service providers to keep your online store secure.

In an era when cyber attacks make news every day, many organizations believe their eCommerce stores are making all the right security moves. But they often overlook certain fundamentals that leave them — and their customers — at high risk.

Rapidly advancing digital customer experience requirements continuously open up gaps between the latest in eCommerce technology and the security needed to make it safe. Today, eCommerce stores are enabling customers to conduct transactions beyond their websites — via mobile and social platforms, for example. Meanwhile, traditional eCommerce sites are being enhanced through integration of collaboration and productivity capabilities, and other increasing uses of APIs. All of this broadens the "attack surface" for eCommerce, potentially making your store more vulnerable.

Here's a rundown of five common — and avoidable — eCommerce security mistakes.

1. Overestimating Application Web-Worthiness

Not every application can withstand the rigors of the web. All too often, companies migrate older applications designed to run on internal servers to the web without properly assessing their online security worthiness.

"We're talking about putting applications and data and infrastructure out on a public website that can be accessed by potentially anyone in the world. Not all applications are designed for that," notes Tim Beerman, Vice President at CenturyLink Business. "A lot of applications are internally designed, and some of them are older and aren't really adequately prepared for the onslaught of threats that can happen over the Internet." As eSecurity Planet put it, web applications "present more security challenges than desktop applications, which are far less accessible and typically have their own unique file formats."[1]

Beerman recommends companies perform a thorough assessment of any application being considered for online customer use. They may be suitable as is, they may need updating, or they may need to be re-imagined in a different model. "You may be better off going with a SaaS version of that application that has better security and other controls built in to its design from the beginning," Beerman says.

2. Taking Risks With Risk Assessment

Risk assessment is expensive and time-consuming, which is why many companies don't do it — or don't do it well. But even if your store is never attacked, blowing off risk assessment may cost you more money in the end.

Such additional cost could be the result of failure to perform the data classification exercise that is a critical element of any thorough risk assessment. Explains Beerman: "If you don't do data classification, then you don't really understand the value of your digital assets. You have to assign a value to your digital assets so you can understand what kind of security controls you will need for each of those assets."

Although data classification categories will vary by industry, they generally follow the pattern seen in this example from Stanford University. It is based on four categories: prohibited, restricted, confidential, and unrestricted, and includes definitions and rules/policies related to each category.

Typically, the more valuable data is, the harder a hacker will try to get at it — and the harder you have to work to keep it secure. Without a data classification exercise, companies end up spending too little or too much to secure data because they're not sure precisely what kinds of controls they need to secure it. But a thorough risk assessment that includes a complete data classification analysis helps to match data assets to the right levels of security and control.

3. Ignoring Middleware Security

Increasing use of cloud computing tends to broaden the eCommerce "attack surface." Noted security experts The SANS Institute states "The increased attack surface in a cloud environment allows for other vulnerabilities to be exploited, thereby increasing the organization's risk. Virtual switches and the hypervisor are two examples of points of attack that are not present in the traditional data center."[2]

This leaves companies vulnerable, especially when building their own private clouds instead of using cloud service providers with extensive cyber security experience. Companies often underestimate the level to which their vulnerability has expanded, especially since so many processes are now automated.

"When you spin up a virtual machine and load a web application, or store data in a database on a server in the cloud, there are a lot of things that humans don't do that have been programmed into the system," notes Beerman. This includes provisioning the right number of virtual machines, grabbing the right amount of storage from the cloud, setting up the network routes, creating virtual Local Area Networks (LANs), and Virtual Private Network (VPN) access.

With all of these configuration management processes comes an increased use of enterprise user portals and APIs, each of which has its own area of potential vulnerability that has to be evaluated and secured. “These are areas that often get overlooked, especially when companies are building their own clouds,” Beerman says.

4. Being a Loner

In the past couple of years, change has come faster and more furiously than ever before. Call it the new normal. And with the ubiquity of powerful mobile and social technology, all organizations — no matter their size or the extent of their eCommerce offerings — must more carefully align cyber security activities with desired business outcomes to ensure the safety of their customers’ transactions and stored data.

This more open, fluid, and interdependent eCommerce environment means that hackers are increasingly using legitimate websites as a means to target victims and distribute malware. “Most web applications have to be fully exposed to the Internet, which makes them easy targets for hackers. The hackers will either break into websites to steal data, or they will use them as a means to distribute malware to other sites.”

In the not-so-distant past, companies were able to depend on signature-based systems to keep them and their customers safe. But with zero-day exploits complicating matters, many of the tools we have come to depend on for security just don’t cut it anymore.

Beerman believes that a key step in taking arms against this sea of troubles is to accept that you can’t do it alone. He recommends moving beyond old notions of security to a new ideal in which organizations work in cooperation with communities of interest, government partnerships, and service providers to assess, plan and, when need be, battle the cyber bad guys.

While there are many organizations working to keep eCommerce secure, here are three top sources of expert and unbiased security information and advice that are worthy of further investigation:

- PCI DSS: Offers a number of documents that provide step-by-step instructions for securing online transactions.
- NIST: Offers a comprehensive framework for improving critical infrastructure cybersecurity.
- OWASP: Its Top 10 Security Project offers insight into the most critical web application security flaws.

5. Mistaking Compliance for Security

Too many companies believe compliance equals security. Or are more frightened about compliance auditors than they are about malicious hackers. But compliance does not make your eCommerce site secure. In the words of leading security provider RSA, “Most compliance mandates reflect best practices that should be interpreted as minimum standards, not sufficient levels, of security.”[3]

“What many companies end up doing is documenting processes and procedures just to meet a certain compliance level, so they can check a box and be done with it. But what companies need is a full risk assessment, and development of policies and procedures to protect data that go beyond the needs of compliance,” Beerman says.

The problem is, regulatory and standards bodies cannot create rules fast enough to keep up with the new possibilities that advancing technology continuously enables — much less any related new threats from hackers. “This is a place where I see a lot of gaps,” Beerman adds.

Conclusion: Constant Vigilance

Securing your eCommerce presence is a daunting task. But taking a cold, hard look at your organization's "attack surface," performing a thorough risk assessment, and participating in security communities of interest can help ensure you avoid the mistakes spelled out in this report. Overall, however, in this time of constant change an old IT best practice is more important than ever before: constant vigilance.

Key eCommerce Security Issues and Actions

- Mobile, social, and cloud technologies are changing the frequency, flexibility, and sophistication of online transactions — and threats.
- Assess apps' "web worthiness" — don't just slap a web label on older applications and infrastructure.
- Do a thorough risk assessment — it might save you money (even in the unlikely event your eCommerce site is never attacked).
- Secure your middleware — it's an increasingly significant concern as more processes are automated through APIs.
- Don't be a loner — join security-related communities of interest and find partners with comprehensive security capabilities.
- Don't mistake compliance for security — there are significant gaps between compliance requirements and modern security threats.

Digital Customer Experience Solutions from CenturyLink

CenturyLink's website hosting, content management system (CMS), and eCommerce solutions are built for global enterprise performance and agile marketing innovation. CenturyLink's solutions accommodate a broad range of website deployments. These include simple, self-managed sites utilizing on-demand cloud infrastructure for short-term campaigns, microsites or development efforts, as well as fully managed production websites that may include CMS and eCommerce platforms hosted on dedicated or hybrid cloud platforms. CenturyLink hosts mission-critical, high-traffic consumer-facing websites and eCommerce sites, including for 30 percent of the Fortune 100. It creates the agile, high-performance digital consumer experience that marketers and eCommerce teams seek, with the control, stability, security, and predictable cost that IT teams demand.

About CenturyLink Business

CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure and hosted IT solutions for enterprise business customers.

For more information visit www.centurylink.com/enterprise.

[1] "Why Are Web Applications a Security Risk?,"eSecurity Planet, September 7, 2012, © 2014 QuinStreet Inc.
http://www.esecurityplanet.com/trends/why-are-web-applications-a-security-risk.html

[2] "An Introduction to Securing A Cloud Environment[end ital], The SANS Institute, © 2012 The SANS Institute, Author Retains Full Rights.
http://www.sans.org/reading-room/whitepapers/cloud/introduction-securing-cloud-environment-34052

[3] "New RSA Security Brief Provides Roadmap for Next Generation Security Operations," RSA, October 29, 2013, © EMC Corporation

Global Headquarters	EMEA Headquarters	Asia Pacific Headquarters	Canada Headquarters
Monroe, LA	United Kingdom	Singapore	Toronto, ON
(800) 728-8471	+44 (0)118 322 6000	+65 6591 8824	1-877-387-3764