Deloitte.

Secure and defend

Addressing the rising tide of cyber security threats in an SAP environment

Exploiting software vulnerabilities is the latest trend in cybercrime—and it can hold big implications for organizations that are built on SAP foundations. As consumer demand for digital engagement has risen, many of those organizations have scrambled to develop and deploy SAP-based applications that connect enterprise resource planning (ERP) platforms through social, mobile, and cloud channels. The result? A potential bonanza for cybercriminals.

Fortunately there is software, such as SAP Fortify by HP and CVA[1] for SAP's ABAP code, designed with advanced capabilities for detecting specific application vulnerabilities—even across a portfolio of hundreds or even thousands of applications. But what happens in the event that the software identifies hundreds of vulnerabilities? Understanding which of these vulnerabilities are the highest risks to your security requires an understanding of the cybercrime landscape, SAP programming and your industry compliance requirements. Deloitte can surgically diagnose the most acute threats to your cybersecurity—and develop a clear plan for addressing them.

Designing awareness

In the sprawl of applications created to make organizations more accessible and improve customer engagement, the software portfolio can become a "system of systems." The challenge becomes especially real in the application-rich, hyper-connected environment in which SAP platforms operate. The potential for inadvertently coding software vulnerabilities is real, and it happens at light speed as organizations rapidly innovate—often focusing more on delivery than on quality. With 84 percent of today's security breaches coming through software,[2] the SAP environment needs heightened vigilance.

The resilience of an SAP software ecosystem depends on the integrity of applications. How well were they built? As a metaphor, take the construction of a new home. The construction materials can be top-notch quality, and the foundation can be solid. However, workers might be required to assemble the materials hastily during construction, or the foundation might shift. Being aware of such problems and addressing them early—during the construction process, before moving in—makes sense. There are three fundamental steps required for such an approach.

Step 1

Diagnosis: Organizations don't have to wait until a system is in production to understand its flaws and vulnerabilities. Tools such as SAP Fortify by HPsoftware give businesses a way to uncover software flaws, gaps, and inconsistencies that can offer openings for hackers. SAP Fortify by HP, paired with Deloitte's secure software enablement (SSE) services, can help diagnose those vulnerabilities during the development process—rather than after you've already placed a system in production. Early diagnosis can save big money. Finding coding structural flaws while an application is under construction potentially can save millions of dollars.

Step 2

Prioritization: It's not enough to know that you have problems with your code as you weave new capabilities into SAP offerings. The challenge is determining how to prioritize the problems you discover. Which assets are most critical? Which problems expose the biggest vulnerabilities? Is the regulatory-compliance factor creating urgency to fix some vulnerabilities ahead of others? How do you make the best use of the resources available to you right now to get started repairing holes? How do you line up the necessary resources to remediate remaining problems?

SSE services can help address such questions—providing emergency remediation to mitigate the most urgent vulnerabilities, taking a strategic approach to addressing the remaining identified vulnerabilities, and putting in place plans for diagnosing and prioritizing future vulnerabilities for your SAP-based landscape.

Step 3

Repair: At the heart of the remediation process is a need to stay ahead of threats—to rapidly secure software and minimize business disruption. To that end, Deloitte's approach to remediation involves providing managed services to fill the skills and experience gaps within an organization, as well as undertaking the development of a comprehensive SSE program that includes policies, procedures, requirements, cross-team integration, and integration on new steps within the software development life cycle.

The approach is one in which developers and security specialists collaborate throughout the entire development life cycle—not just at the post-production maintenance phase. Security and design teams work together to plan, model, review, test, and fix software from the very beginning of projects.

[1] SAP NetWeaver Application Server, add-on for code vulnerability analysis (CVA).
[2] 2014 Ponemon Report on Global Cyber Crime, sponsored by HP Enterprise Security, independently conducted by Ponemon Institute LLC, October 2014.

A better system

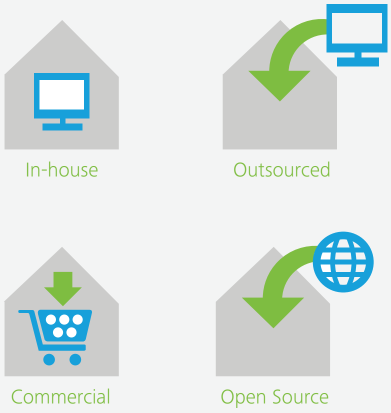
Deloitte's early-detection approach to software vulnerabilities in the SAP realm brings with it many benefits besides the obvious potential cost savings. The approach makes the unknown known—and it makes it known earlier. It puts application security measures into action to help identify code problems before they become bigger problems, and by addressing problems before they go live, it closes the window of opportunity for hackers—helping organizations prevent attacks that can lead to business disruptions.

When paired with a broader security plan—one that emphasizes post-production activities such as preparing for inevitable security breaches—the early-detection approach can help transform businesses into not just secure organizations but resilient organizations. Organizations that approach IT security from only a traditional standpoint—failing to consider the unique challenges associated with SAP—stand to leave considerable vulnerabilities unresolved. An investment in SAP digital-based capabilities requires an investment in a risk prioritized approach to SSE.

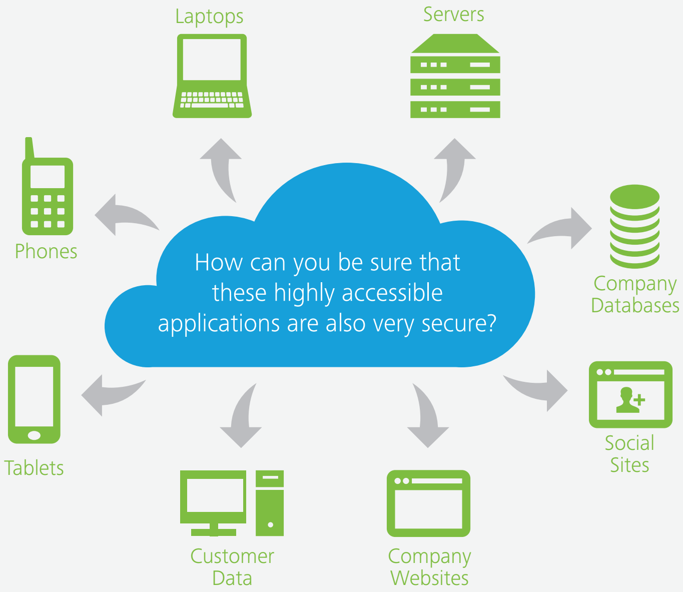
To find out how Deloitte's SSE capabilities, coupled with SAP Fortify by HP, can help your organization become a more vigilant, secure, and resilient enterprise, all it takes is a conversation. Contact us to get the conversation started. We can provide additional information, insights, and a consultation to help sharpen your focus on the challenges associated with SAP and secure software enablement.

Understanding the challenge

1 Software originates from many different sources.



2 Applications integrate to many types of technologies through many different channels.



Contact

Mike Kosonog
Partner
Cyber Risk Services
mkosonog@deloitte.com

Ben Anderson
Senior Manager
Cyber Risk Services
benanderson@deloitte.com

Mark Moore
Senior Manager
Cyber Risk Services
marmoore@deloitte.com

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.