pwc | Switzerland

Why should you care about vulnerability management?

22 Jan 2021

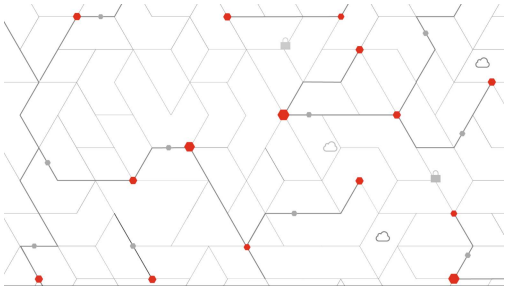
by Fabian Faistauer
Cyber Compliance Monitoring, Director, PwC Switzerland

In such a fast-paced, IT-dependent business world, bugs almost inevitably creep in. In the worst case they can be exploited by malicious actors to compromise the confidentiality, integrity or availability of your systems. Under these circumstances you can't afford to leave security to chance. You must identify and quantify the vulnerabilities and manage them effectively to avoid damage to your reputation and bottom line.

Massive breaches have reminded many companies of the huge risk IT vulnerabilities pose and have prompted them to take firm, proactive action to manage them. But with increasingly complex infrastructures – also encompassing the cloud – it's hard to keep track of all the rapidly growing vulnerabilities. This is good news for cybercriminals, who have learned how to exploit these weaknesses for malicious ends.

There's also regulatory pressure to respond to these threats. For example, the Swiss regulators require organisations providing IT services in the finance sector to have a risk-based vulnerability management programme in place. With digital and cloud-based solutions on the rise in all areas of business and life, we're sure to see more regulation going forward.

A growing number of companies are realising the need to identify and manage their IT vulnerabilities, and COVID-19 has merely heightened the urgency. In the Swiss sample of PwC's Digital Trust Insights 2021 survey, 36% of respondents said that the pandemic is likely to lead to better and more granular quantification of cyber risk. Though some companies are already acting on this, many still haven't put their plans into action or have no plans at all in this area.



2021 Global Digital Trust Insights

What Swiss business and technology experts expect in the coming months.

Read it here

What is vulnerability management?

Let's assume you're one of the companies weighing up their options. To get to grips with vulnerability

up their options. To get to grips with vulnerability management you first have to understand 'vulnerability' in the context of your IT infrastructure. Vulnerabilities are bugs that can be exploited by people with malicious intent to circumvent security controls and gain access to your systems and data.

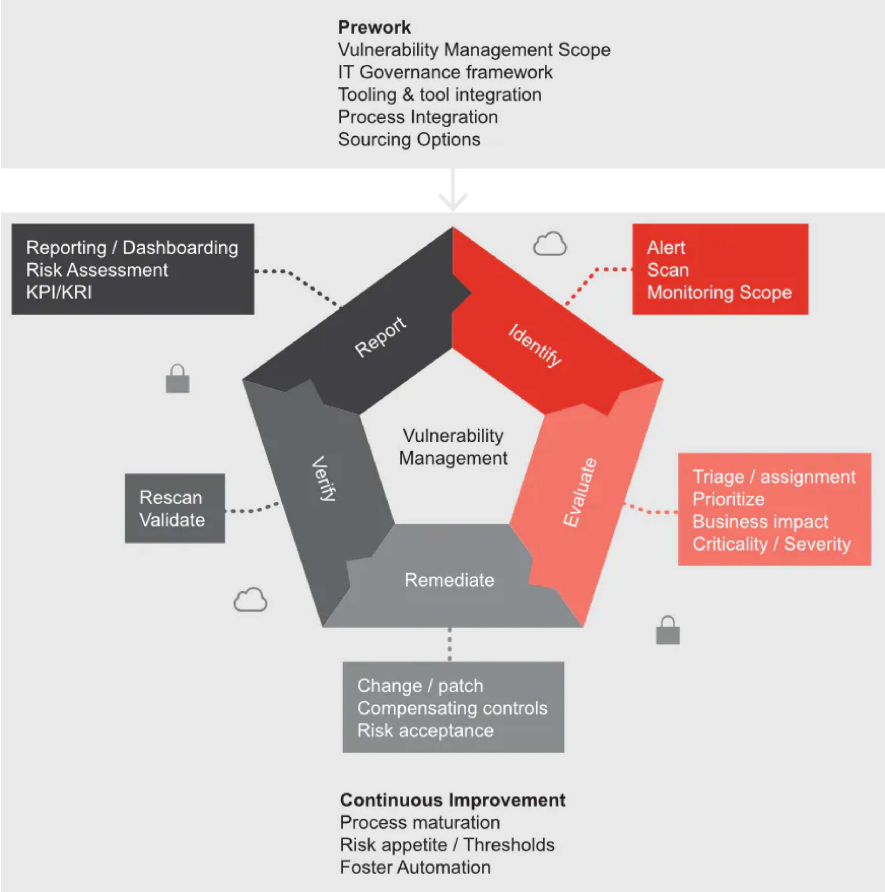
The aim of vulnerability management is to identify and remediate known vulnerabilities and assess how able and mature your IT organisation is when it comes to applying security patches within a defined time objective. Vulnerability management is an ongoing process of identifying, evaluating, remediating, verifying and reporting vulnerabilities in IT systems and the software which runs on the IT infrastructure.

In addition to boosting your company's cybersecurity and reducing the risk of expensive and embarrassing breaches, effective vulnerability management assures adherence to security requirements and regulatory compliance. The regulations affecting companies in Switzerland include those issued by **FINMA**, **EU-GDPR**, SWIFT, **PCI DSS** and in relation to the electronic patient dossier (**BAG TOZ**). As we said before, this list is likely to grow as reliance on digital solutions increases in all areas of life and business.

The vulnerability management process

Now let's take a more detailed look at the actual process of vulnerability management. As we've said, the ultimate aim is to achieve a sustainable and mature security level within the enterprise by proactively identifying and remediating vulnerabilities, while at the

same time complying with ever-increasing regulatory requirements. This is best achieved in a cycle consisting of various components.



Prework: Defining the scope of vulnerability management, establishing IT governance with roles and responsibilities, having vulnerability management as an integrated process in IT service management, and evaluating sourcing options.

Identify: Setting up a central asset inventory and defining the right scanning method. Which assets should be scoped in? Which assets are critical IT assets that hold sensitive data?

Evaluate: Assessing the company-specific environmental characteristics: the context of the vulnerabilities on the asset; criticality and severity of the vulnerabilities; the risks that are relevant to the organisation.

Remediate: Addressing vulnerabilities once they're found. How effective is the patch management process? Can compensating measures be applied via formal change management? Does the organisation accept the residual risk if patching is not available or possible?

Verify: Doing a timely rescan, periodic reviews and ensuring an escalation process is in place to deal with vulnerabilities.

Report: Communicating with the respective line of defence by means of stakeholder-specific reporting (dashboard overview).

Continuous improvement: Review the lessons learned, evaluating your risk appetite (risk tolerance), reviewing the maturity of the process, improving continuously by means of an automated process, and increasing maturity.

How to address the challenges

An approach built on three pillars – IT governance,

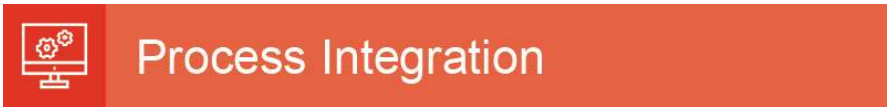
process integration, and tooling and tool integration – provides a solid foundation for embracing vulnerability management. The precise steps will depend on your existing set-up and what's in place already. But to give you an idea of what might be involved, here are a few examples of challenges that we have helped clients address.

1) IT Governance: Vulnerability management needs established IT governance to identify what IT assets are in scope and clearly define roles and responsibilities for compliant data processing.

Client challenges addressed:

No active vulnerability management for the timely remediation of vulnerabilities (lack of clear definition of roles and responsibilities).

No clear ownership and mapping to service criticality of configuration items and IT assets.



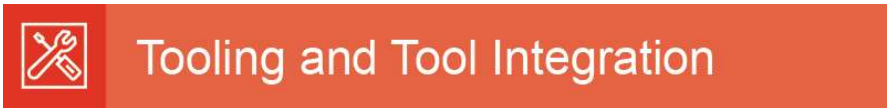
2) Process Integration: Vulnerability management requires a process framework: a different angle on IT monitoring, event management and incident response. Compliance needs to be managed by defining technical standards and systematically monitoring compliance with the IT standards.

compliance with the IT standards.

Client challenges addressed:

No sustainable integration of IT security and IT service management in a process framework aligned with business context.

Agree on applicable patch cycles for each technology and verify that the relevant patches are applied within the defined timeframe.



3) Tooling and Tool Integration: To get the best value and benefit from the vulnerability scanning tools, they need to be integrated. Consider combining vulnerability scanning tools with an orchestration solution for seamless integration with your IT service management system and IT asset register/CMDB, and use automation capabilities and play books rather than designing workflows in many different tools.

Client challenges addressed:

High level of manual effort involved in managing vulnerabilities.

Lack of integration with IT asset register, critical system inventory, IT service

management tool for incident management and change management tool.

To sum up: it's time for you to invest in vulnerability management

IT vulnerabilities give attackers an open door to your organisation. The fact that these vulnerabilities are complex and rapidly changing makes them an even greater risk and difficult to address. Just as people delegate their virus defences to companies specialising in antivirus software, you're not on your own when it comes to managing IT vulnerabilities either. There are specialists out there who can help to make sure you have effective vulnerability management in place that keeps pace with the threats – protecting your business and your customer data, and ultimately building precious trust.

Any questions?

Reach out to us

Share this page:

Contact us

Fabian Faistauer

Cyber Compliance Monitoring, Director, PwC Switzerland
Tel: +41 58 792 13 33
Email

Lorenz Neher

Head Security Architecture and Operation, PwC Switzerland
Tel: +41 58 792 47 85
Email

Robin Attinkara

Cyber Compliance Monitoring, PwC Switzerland
Tel: +41 58 792 24 27
Email

Global Markets
Legal
People and Organisation
Private Wealth
SME and Family Business
Tax Advice

Industrial Manufacturing
Real Estate
Retail and Consumer Goods
Pharmaceuticals and Life Sciences
Sports Business Advisory
Technology, Media and Telecommunications

Customer Centric Transformation
Cybersecurity
Data & Analytics
Experience Consulting
The Difference

Code of Conduct
Reports
Corporate Responsibility
Our History
Alumni

Apprentices
PwC as an Employer
PwC's Career Blog