ActualTech MEDIA

Hewlett Packard Enterprise

Staying Ahead of Security Threats

Ed Tittel

CONTENTS

IN THIS PAPER

This tech brief looks at how HPE and its partners help small to mid-size businesses keep out of security trouble. Such operations must be able to identify threats and vulnerabilities that pose potential risks, prioritize them by severity, and set up risk mitigation and action plans to address them. This involves constant, ongoing effort to keep up with an ever-changing threat landscape.

Highlights include:

- Aligning security strategy with business objectives
- Building a security-first business culture
- Monitoring attack surfaces and proactively remediating before hackers can strike

When it comes to cybersecurity, the old saying “An ounce of prevention beats a pound of cure” is particularly apt. That’s because the costs of a cure—remediating the consequences of a security incident or breach—are high enough nowadays to pose an existential threat to most businesses, especially smaller operations.

That’s what makes understanding and anticipating the dangers that security threats and vulnerabilities can pose so important, if not downright essential. Ultimately, it’s all about risk management, which means the following:

- As threats and vulnerabilities make themselves known, the first step is to **identify** those that pose actual risks to the business, and to assess their potential impacts and consequences.
- For those items where risk is involved, it’s essential to **prioritize** them so that those with the highest costs or most dire consequences are addressed first, and so on, in decreasing order.
- For items with sufficient risk to warrant a response, businesses should set up **risk mitigation and action plans** to address them.

In practice, especially for businesses too small to implement a security team in-house, this means subscribing to a threat intelligence and remediation service of some kind. In fact, HPE and its partners can help with such things, including identification, prioritization, and remediation of risks as part of a comprehensive security service offering.

The Cloud Changes Everything … Including Security

As organizations bring cloud subscriptions and services, new and challenging threat vectors will also come into a business’s security picture. This makes it vital to up the security game, and to take steps to improve the organization’s security posture and cyber resilience. The following business exercises should be undertaken to help businesses achieve those goals:

- **Align your security strategy with your business priorities:** By understanding the gaps between business and cybersecurity priorities, management and stakeholders can commence aligning both strategies to ensure key priorities are focused, and resources and budgets allocated accordingly. It’s important that business leaders reach a state of agreement on the priorities and that risk profiles are understood clearly.
- **Build a security-first culture:** Prioritizing a security-first culture is an important step to thriving in a world rife with uncertainty and risk. Protecting vital assets becomes everyone’s business. It’s essential to invest in staff awareness training given its prominence as a source of cyber risk, and because a collective effort against cyberthreats will better serve your business.
- **Know your attack surface and fix vulnerabilities before hackers find them:** Cyber vulnerability analysis, also called security testing or pen testing, is a process of testing to assess your organization’s security posture (see **Figure 1**). It identifies vulnerabilities before an attacker can exploit them. This process provides insights into the risks that organizational assets face, from external and internal perspectives. It also helps identify potential security gaps prior to formal compliance assessments or audits. To enhance security posture in your organization it’s also important to develop actionable mitigation plans. To that end, engaging experienced partners (such as HPE and its partners) can bridge cyber skills gaps in your business and mitigate vulnerabilities.

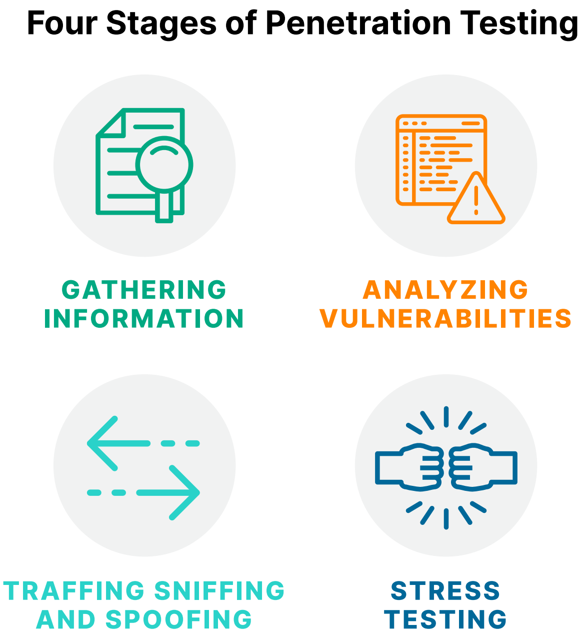
Four Stages of Penetration Testing
GATHERING INFORMATION
ANALYZING VULNERABILITIES
TRAFFING SNIFFING AND SPOOFING
STRESS TESTING

Figure 1: The four stages of penetration testing, also known as pen testing

Terminology Explainer

Disaster recovery: Describes services and systems that permit a business to return to normal operation even in the face of disaster or a total interruption of access and service.

Ransomware: A type of malware that denies businesses access to their systems and data by encrypting everything, so that nothing will function. Crooks claim that paying a ransom will return everything to a pre-attack state, but the FBI recommends against paying ransoms because that isn't always how things turn out.

Virtualized and containerized apps and data: Applications and data that run in virtual machines or containers, often in the cloud, typically as part of a usage- and consumption-based computing model.

Edge to cloud: Refers to computing resources and data that may reside in datacenters or server rooms on-premises at the business core, at the network edge in remote of field locations, or on one or more cloud platforms (e.g. Amazon Web Services, Microsoft Azure, Google Cloud Platform).

Hybrid and multi-cloud scenarios: A hybrid cloud involves integrating local and cloud-based computing resources into a single environment for handling computing tasks. Multi-cloud means the same thing, except it involves two or more cloud platforms. Most modern businesses operate in hybrid multi-cloud environments, and seek to position workloads and data where they make most sense from a cost, security, and performance perspective.

> It's important that business leaders reach a state of agreement on the priorities and that risk profiles are understood clearly.

How HPE (and Partners) Can Secure IT

As a quick examination will verify, HPE's cybersecurity solutions are comprehensive, innovative, and robust. Its security capabilities begin at the hardware level and extend all the way to users and systems at the network edge. The overall thrust is to gather and analyze security intelligence to keep up with the threat landscape, to secure systems and services in business use, and to advise (and assist) its customers in managing and minimizing security risks.

> HPE's cybersecurity solutions are comprehensive, innovative, and robust. Its security capabilities begin at the hardware level and extend all the way to users and systems at the network edge.

HPE SECURITY STARTS WITH ITS SERVERS

HPE is recognized as a purveyor of the world's most secure industry standard servers. Its ProLiant server family has won numerous awards and accolades, thanks to these specific characteristics:

- **Protect:** Systems avoid hardware- and firmware-level exposure to attack via a silicon root of trust, trusted platform module (TPM) enhancements, multiple levels of tamper-proofing, and added HPE innovations such as "Integrated Lights Out" (iLO) firmware to promote "security-first" capabilities.
- **Detect:** A whole suite of innovations detects and fends off threats during runtime, including boot integrity checks, whereby iLO wipes potentially (or actually) hacked firmware code and replaces it with a known valid copy if possible. If repair proves impossible, systems won't be allowed to boot (provides pre-boot protection against rootkits and other insidious firmware-based attacks).

- **Recover:** Robust capabilities to restore and recover systems back to their last known, good, working states quickly and easily, thanks to tamper-proof, encrypted backups and safe, secure restore mechanisms.

Zerto

In 2021, HPE completed acquisition of Zerto, a company that specializes in disaster recovery, ransomware recovery, and multi-cloud mobility solutions. Now part of HPE, Zerto offers continuous data protection and recovery for virtualized and containerized apps and data from edge to cloud. With Zerto, organizations can recover in minutes to a state seconds before an attack, eliminating lengthy and costly disruption and data loss. Zerto brings increased availability with a much lower administrative overhead than legacy data protection solutions. In addition, Zerto's unified, scalable, and automated data management makes workload and data mobility across clouds easy and straightforward. Furthermore, Zerto offers continuous data protection for organizations employing a hybrid-cloud strategy and includes Disaster Recovery as a Service (DRaaS) with a network of over 350 managed service providers. Visit the HPE/Zerto page to learn how your business can avoid data losses and application downtime as close to zero as technology can get.

HPE SECURITY SOLUTIONS

HPE's security tools, technologies, and solutions all employ three key approaches throughout their design, development, manufacture, and maintenance. These are best described as follows:

- **Data-centric security:** Security measures seek to protect data first and foremost, particularly data with any kind of sensitivity (personally identifiable information, or PII; accounts and passwords; financial, health, or other legally protected data, and so forth). This ties directly into the next approach, which focuses on who gets access to systems and data, and for what purposes.

> Engaging experienced partners (such as HPE and its partners) can bridge cyber skills gaps in your business and mitigate vulnerabilities.

- **Zero-trust security:** The National Institute of Standards and Technology (NIST) describes zero trust (ZT) with the epigram: "Never trust; always verify." ZT focuses on data and service protection but should also include all assets (devices, infrastructure elements, applications, plus virtual and cloud resources) and subjects (users, applications, services, and systems). Basically, ZT assumes attackers are always present and active. Thus, it extends no implicit trust to anyone, and always analyzes and evaluates risks to assets and business functions. Verifying identity for all access requests is a key strategy, as is applying the "Principle of Least Privilege" (aka PLP), which means allowing no more privileges than those necessary to subject than they need to do their jobs.
- **DevSecOps:** Simply put, this is an extension of the idea of DevOps, which puts developers (and support personnel such as testers, documenters, and trainers) together with operations staff (administrators, tech support, and field technicians or troubleshooters) into a single organization with shared goals and objectives. DevSecOPs goes one step further and integrates the security team across the entire development lifecycle, so that security is considered during design, construction, testing, maintenance and retirement phases in business IT operations.

BEYOND THE SOLUTIONS: EXPERT CONSULTING HELP

HPE Pointnext Services can help small to midsize businesses audit, define, and refine their security strategies. Pointnext offers expert assistance in formulating security policy, and meeting compliance requirements for privacy, confidentiality, and data protection. They can also help resource- or knowledge-constrained businesses integrate affordable, effective solutions for business continuity and disaster recovery. In fact, Pointnext specializes in helping businesses prepare security blueprints to ground security designs and implementations firmly in reality (and within budgetary constraints). They can also provide end-to-end assistance through test, pilot, and production deployments. Ultimately, Pointnext can help businesses ensure that security gets embedded across the whole organization: remote workers, at the edge, on-premises, and in hybrid, multi-cloud environments.

Securing the Supply Chain

HPE operates a Trusted Supply Chain (TSC) to serve customers with stringent, higher-than-normal security requirements or usage scenarios. Representative customers from this supply chain include U.S. government and public sector organizations and agencies who must acquire made-in-USA products with verifiable product assurance. Security goes into the TSC in two important ways. First, such products include hardened security features designed to make them tamper-resistant, if not tamper-proof. Second, HPE supervises the entire supply chain, and approves all parts, observes assembly, and keeps packaged goods secure (and tamper-free) until customers accept delivery.

Project Aurora provides a complete security architecture with new embedded and integrated security solutions starting at the at the silicon level. Learn how Project Aurora is ignited in the supply chain and establishes an immutable chain of trust up through the infrastructure, operating system (OS), software platform, and workloads without requiring signatures, significant performance trade-offs, or lock-in.

> **HPE's security tools, technologies, and solutions all employ three key approaches throughout their design, development, manufacture, and maintenance.**

HPE and its partners offer a broad range of carefully crafted security solutions to help small to midsize businesses manage risk, protect their systems and data, and cope with today's complex and forbidding security landscape. Visit the HPE Small and Midsize Business IT Solutions page for all the details. Consider further that HPE and its partners can also offer coaching, consulting, assistance, and services to help smaller businesses stay safe and secure through its Pointnext services organization.