CYBERSECURITY 101 · eBuilder Security

Vulnerability Management

Every organisation runs software with flaws. Vulnerability management is how you find the ones that matter and fix them before an attacker does.

WHAT IT IS

Vulnerability management is the continuous loop of finding security weaknesses across your systems, prioritising them by real risk, fixing or reducing them and verifying the fix. It runs for as long as your systems exist, because new flaws appear daily. It is now the front line of defence, not an IT footnote.

WHY IT MATTERS

31%

of breaches now begin by exploiting a vulnerability, the top initial access vector

Verizon DBIR, 2026

43 days

median time to fix a known-exploited flaw, while attackers exploit new ones in days

Verizon DBIR, 2026

40,000+

new CVEs published in 2024, up from about 28,000 in 2023

NIST NVD, 2024

WHAT HAPPENED

In 2017 the credit agency Equifax was breached through a critical Apache Struts flaw (CVE-2017-5638). A patch had been available for about two months, but an internal scan missed the vulnerable system and the alert to patch never reached the right team. Attackers reached the data of roughly 147 million people. Source: US Government Accountability Office.

RED FLAGS TO WATCH FOR

Signs your vulnerability management is not keeping up:

- You do not have a live inventory of your internet-facing systems
- You scan a few times a year rather than continuously
- Findings pile up with no owner and no deadline
- You prioritise by CVSS score alone, ignoring what is actually exploited
- Fixes are marked done but never rescanned to confirm they landed

> THE ONE RULE THAT STOPS IT
>
> **Fix what attackers are actually exploiting first, then rescan to confirm it is gone. Do not try to patch everything.**

THEN BUILD THE HABIT AROUND IT

- Keep an accurate, continuous inventory of assets and exposed services

- Use authenticated scans for anything you own
- Prioritise with exploitation data, such as CISA's Known Exploited Vulnerabilities list
- Give critical internet-facing flaws a deadline measured in days
- Verify every fix by rescanning, then track how fast you close flaws

MYTHS AND FACTS

MYTH

Vulnerability management is just running a scanner.

FACT

Scanning is only the first step. The value is prioritising, fixing what matters and verifying the fix.

MYTH

If we patch everything, we are safe.

FACT

No team can patch everything. Prioritising by real exploitation beats chasing every CVE.

MYTH

A high CVSS score always means fix it first.

FACT

Severity is not risk. A flaw only matters if it is reachable and being exploited.

THE LEGAL DUTY

For Swedish organisations this is now law. NIS2, transposed as Cybersäkerhetslagen (in force 15 January 2026), requires continuous monitoring and vulnerability handling under Article 21, with the board accountable under Article 20. DORA and ISO 27001 expect the same discipline.

GET HELP

eBuilder Security runs vulnerability management as a managed service for Swedish organisations, from continuous scanning to prioritisation and remediation tracking.

Read the Full Article →