CORPORATE AUDIT

Unpatched Flaws Are Now the Most Common Way into a Breach, Verizon Finds

On 19 May 2026, Verizon published this year’s Data Breach Investigations Report (DBIR). For the first time in the report’s history, exploiting a vulnerability overtook stolen credentials as the most common way into a breach. In the cases it analyses, attackers got in more often through an unpatched software flaw than with a stolen password.

The headline finding is in Verizon’s press release of 19 May 2026.
https://www.verizon.com/about/news/breach-industry-wide-dbir-finds

According to Help Net Security’s summary of the report, fixing has also slowed down. The median time from detecting a vulnerability to patching it fully rose from 32 to 43 days. For as long as that gap lasts, the flaw stays open to anyone looking for it.

The remediation figures appear in Help Net Security’s summary of 20 May 2026.
https://helpnetsecurity.com/2026/05/20/verizon-2026-dbir-findings

Two Cases in Colombia and Mexico with No Sophisticated Malware

On 21 July 2026, Kaspersky published two ransomware cases that its incident response teams investigated at unnamed companies in Colombia and Mexico. According to Kaspersky, in neither case did the attackers rely on sophisticated malware. In Colombia, the attackers came in through a remote desktop service exposed to the internet. In Mexico, they used a misconfigured database server reachable from the internet, with credentials that sat in code published on GitHub. Kaspersky adds that the Mexican attack began about three months before it was detected, and that alerts were raised but nobody investigated them. In both cases the encryption used features built into Windows, and the ransom notes came out of the office printers.

The technical analysis was published on Securelist, Kaspersky’s research blog, on 21 July 2026.
https://securelist.com/new-extortion-scheme-printers-bitlocker/120718/

A Useful Benchmark: CISA’s Directive on Edge Devices

On 5 February 2026, the US agency CISA issued Binding Operational Directive 26-02. It requires US federal civilian agencies to inventory edge devices that no longer receive vendor support

(firewalls, routers, switches, load balancers, wireless access points) and to remove them in stages: after 12 months, those already out of support by then, and after 18 months, all those identified. CISA says it is aware of widespread exploitation campaigns against these devices. The directive does not apply to any Venezuelan business. Its reasoning still works as a benchmark: a device out of support will not get the patch for its next flaw.

The full text is on CISA's directive page of 5 February 2026.
https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices

What to Check in Your Business This Week

- List everything that faces the internet (firewall, VPN, router, NAS, remote desktop, admin panels, the website and its panel) and record each item's model, version, who maintains it and until when the vendor publishes updates.
- Look up each vendor and product in CISA's Known Exploited Vulnerabilities (KEV) catalogue, and move anything listed there, or out of support, to the front of the queue.
- Set a maximum time for applying critical fixes to those devices and record the actual date of each patch, so you know your own patch time from your own data.
- Take remote desktop and databases off the internet; if remote access is needed, route it through a VPN with two-step verification.
- Search the code your business or its suppliers have published on GitHub or similar services, and documents shared by public link, for passwords or keys; if one turns up, change it first and remove the file afterwards.
- Name one person who receives firewall, antivirus and sign-in alerts, with set hours and clear instructions on what to do with each one.

How We Work Through It in Security Audits & Penetration Testing

We start with a written scope and signed authorisation: which addresses, domains and devices belong to the business, which tests are agreed and when they may run. Then we review the external exposure as anyone on the internet would see it: open services, versions, admin panels, remote access and devices out of support. We compare each item with CISA's KEV catalogue and its vendor's support dates, and we search public code and exposed documents for the business's credentials.

Authorised tests confirm what is actually reachable and exploitable, and are planned so as not to disrupt operations. Every finding comes with its evidence. The executive report ranks fixes by exposure and known exploitation as well as technical severity, and names the unsupported devices

worth replacing. Once your team has made the changes, we test again to confirm each fix works.

> *An audit describes what was found within a scope at a particular date. It cannot guarantee that no other vulnerabilities exist, and it does not replace ongoing updates, which also depend on the vendor continuing to publish patches. The figures cited come from Verizon and Kaspersky and describe the cases those companies analysed.*

A Check You Can Run

Open the administration page of your main firewall, VPN or router and note its model and firmware version, without changing any setting. Look up that model on the manufacturer’s support site to see whether it still receives updates and until when. Then search the vendor and product name in CISA’s Known Exploited Vulnerabilities catalogue. If the model is out of support, or the catalogue lists a flaw in that product and the vendor’s advisory shows that your version is affected, that device goes first on the list to patch or replace.

Supporting guidance: CISA’s Known Exploited Vulnerabilities catalogue.
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Continue with: The Old Website Nobody Remembers May Still Be Online.
https://systems.kavaliero.com/en/blog/the-old-website-nobody-remembers-may-still-be-online

For help with this work, see the scope of Security Audits & Penetration Testing.
https://systems.kavaliero.com/en/services/security-audits