Latvia's 2026 **Threat** *Picture*

6 MOVES TO MAKE THIS QUARTER

offseq

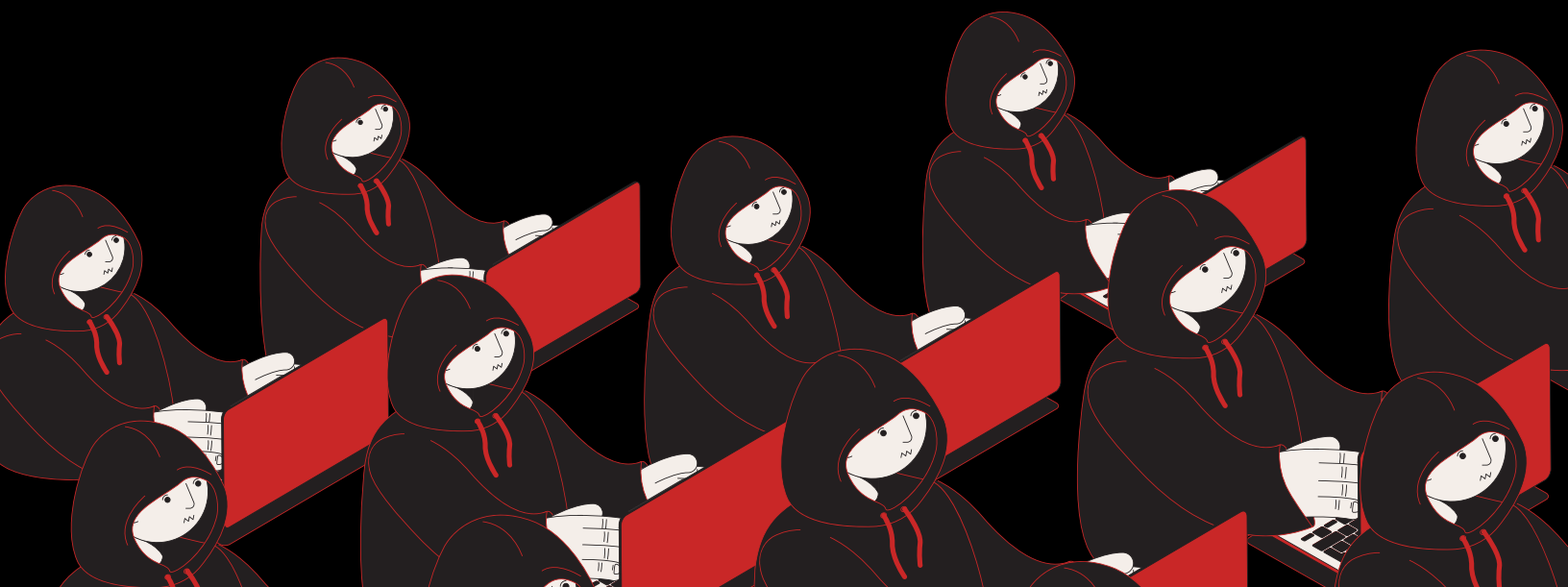
Introduction

Every quarter, CERT.LV publishes the closest thing Latvia has to a national cyber weather report. The Q1 2026 numbers are not reassuring — but they are useful, because they point to something practical: the gaps attackers exploit most are the ones organisations can actually close.

The headline is stark. CERT.LV recorded **757,286** compromised devices in Latvian cyberspace —

the highest figure ever recorded — and the majority are configuration weaknesses: systems left exposed, misconfigured or unpatched, driven largely by human factors and insufficient security standards. Since Russia's full-scale invasion of Ukraine in 2022, registered incidents have risen sixfold and compromised devices eightfold.

At OffSeq, we test Latvian and European organisations the way real attackers do — and we see exactly what that national statistic describes, every week. This briefing translates the latest data into six concrete moves your organisation can make this quarter. None of them costs more than a breach.



757,286 compromised devices in Latvia — a record high (CERT.LV, Q1 2026)

The majority are configuration weaknesses — exposure and misconfiguration, not exotic zero-days

846 incidents handled manually by CERT.LV in Q1 2026 — the second-highest quarter on record

6× more incidents · 8× more compromised devices than before 2022

Supply chain & external providers — now the most common backdoor into organisations

AI is accelerating attacks — faster, more automated, increasingly social-engineering-led

FROM OFFSEQ'S FRONT LINE

This isn't theoretical for us. In a single recent month, OffSeq responsibly disclosed 9 vulnerabilities through CERT.LV's Coordinated Vulnerability Disclosure (CVD) programme — 5 of them rated critical — affecting Latvian essential and important entities, including critical infrastructure. The "configuration weakness" in the national data isn't an abstraction to us; it's what we find and report, before an adversary reaches it first.

The six moves

01 Find the misconfigurations before attackers do

The single biggest category in the national data isn't sophisticated malware — it's exposure: forgotten services, misconfigured systems, expired certificates, weak settings. You cannot fix what you cannot see. Map your real external attack surface — every domain, subdomain, exposed service and piece of shadow IT — and keep watching it, because it changes daily.

- Inventory everything internet-facing, not just what you assume is in scope
- Hunt for misconfigurations, exposed admin panels, leaked files and outdated components
- Re-check continuously — exposure drifts every time a system changes

EXPERT INSIGHT

OffSeq Guard continuously maps web exposure across our monitored estate (113 countries) with daily drift detection, and our Attack Surface Management and Security Audit services turn that visibility into a prioritised, fix-it-first list.

02 Shut the door on weak and stolen credentials

Stolen and reused passwords remain one of the most reliable ways in. Globally, the most common passwords are cracked in under a second, and the great majority of people reuse credentials across accounts — so one leak quietly becomes many break-ins. Assume your users' passwords are already circulating, and design for it.

- Enforce multi-factor authentication everywhere it matters — email, VPN, admin and finance first
- Block weak and previously-breached passwords; favour long passphrases over forced complexity
- Monitor the dark web for leaked credentials tied to your domains — and reset fast when they appear

EXPERT INSIGHT

OffSeq Breach scans roughly 2.7 million leaked credentials every week for exposure linked to client domains, so you hear about a leak before an attacker puts it to use.

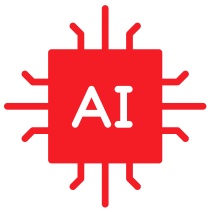
03 Treat your supply chain as part of your attack surface

CERT.LV is explicit: external providers and supply chains are now the most common backdoor into organisations. Your security is only as strong as the vendors with access to your systems and data — and under NIS2, that exposure is your responsibility, in writing.

- Map which suppliers touch your systems, your data and your identities
- Put cybersecurity requirements in contracts — and verify them rather than assume them
- Monitor your key suppliers' exposure and breach status, not only your own

BEST PRACTICE Use OffSeq Breach and Guard to keep watch on critical suppliers' exposure, and our NIS2 & ISO 27001 Readiness service to put the supply-chain clauses and evidence in place that your auditors will ask for.

04 Prepare your people for AI-grade social engineering



The newest shift in the data is AI: attacks are now faster, more automated and increasingly social-engineering-led — from convincing phishing at scale, to deepfake voice calls, to prompt-injection against the AI tools your teams are adopting. Technology alone won't stop this. Trained people will.

- Run realistic phishing, vishing and — now — prompt-injection simulations, not slideshows
- Teach staff to verify any unusual request through a second, independent channel
- Make reporting a suspicious message easy, fast and blame-free

EXPERT INSIGHT

OffSeq's Awareness Lab drops staff inside live phishing, voice-scam and AI prompt-injection simulations, and our Employee Awareness Training and Social Engineering Assessment test whether the lessons actually hold under pressure.

05 Move from annual snapshots to continuous visibility

The clearest message in the data is pace: attacks keep getting faster and more automated. A once-a-year penetration test and a static report no longer reflect your real risk on any given day. Resilience comes from continuous visibility — knowing what changed and what's newly exposed, as it happens.

- Monitor your attack surface and credentials continuously, not annually
- Track new, relevant vulnerabilities against the technology you actually run
- Re-test after every significant change — and verify that fixes genuinely worked

SOLUTION OffSeq Radar tracks more than 100,000 vulnerabilities across 191 countries, ranked by real-world exposure, while Guard's drift detection flags new exposure the day it appears — so your attention goes to what matters now.

06 Make sure you can report an incident within 24 hours

When something does happen, the clock is short: NIS2 requires an early warning within 24 hours of becoming aware of a significant incident. The time to write — and rehearse — your incident-response plan is now, not in the middle of the breach.

- Document who does what, who decides, and who communicates
- Pre-build your NIS2 reporting workflow, templates and contacts
- Rehearse it — a plan you have never tested is a plan you don't really have

ONGOING SUPPORT

OffSeq builds and rehearses NIS2-aligned incident-response plans, and our CISO-as-a-Service provides the accountable security leadership the law now requires, without the cost of a full-time hire.

Conclusion

The Q1 2026 data is a high-water mark, but it isn't a mystery. The same handful of gaps — exposure, credentials, suppliers, people, pace and readiness — account for most of what goes wrong. Close them, and you move from an easy target to a hard one. OffSeq exists to find those gaps the way an attacker would, and to help you close them before they're used against you.

See how you'd actually be attacked — and how to hold the line.

Scope a test, run a free maturity check, or book a consultation. 24-hour reply.

Book a consultation →

offseq

Our Services:

- CISO-as-a-Service from €149 per month
- Comprehensive Risk Assessments
- Customized Employee Cybersecurity Training
- Incident Response Planning and Compliance Support

Contact us today for a complimentary consultation:

www.offseq.com root@offseq.com

Secure your business future with confidence — partner with OffSeq today.

offseq