

Checklist

5 signs your organization is exposed to risk without knowing it

mtp DIGITAL BUSINESS ASSURANCE

Checklist | 5 signs your organization is exposed to risk without knowing it

For years, many organizations have focused their security strategy on identifying technical vulnerabilities. However, today's digital environment has changed radically, and risk exposure no longer depends solely on the existence of vulnerabilities, but on how they combine with the attack surface, the available access and the criticality of assets.

This checklist helps identify early signs of risk exposure that many organizations still do not see.

1. THERE IS NO COMPLETE INVENTORY OF DIGITAL ASSETS

Many organizations lack clear visibility into all the assets that make up their digital ecosystem.

This includes:
- On-premise systems
- Cloud services
- SaaS applications
- APIs exposed to the internet
- Third-party integrations
- Identities with access to critical resources

When there is no up-to-date asset inventory, it is impossible to truly understand the organization's attack surface.

Key questions:
- Do we have visibility into all assets exposed to the internet?
- Do we know which applications are connected to our critical systems?
- Is it clear to us who is responsible for each asset?

2. VULNERABILITIES ARE PRIORITIZED BY TECHNICAL SEVERITY ALONE

Many organizations prioritize vulnerabilities using technical metrics such as CVSS. However, technical severity does not always reflect the real risk.

For example:
- A critical vulnerability in an isolated system may represent a low risk
- A medium vulnerability in a critical system exposed to the internet may represent a high risk

Without business context, organizations may spend time solving problems that do not significantly reduce their exposure.

Key questions:
- Do we prioritize vulnerabilities based on the criticality of the asset?
- Do we understand which vulnerabilities can affect critical business processes?

3. SECURITY IDENTIFIES PROBLEMS BUT DOES NOT CONTROL REMEDIATION

In many organizations there is a clear separation between those who identify risks and those who must resolve them.

The security team identifies vulnerabilities, but remediation depends on:
- Infrastructure
- Cloud
- Development
- Operations

When there is no clear process for prioritization and coordination, many vulnerabilities remain open for long periods.

Key questions:
- Is there a clear risk remediation process?
- Are specific owners assigned to resolve critical vulnerabilities?

4. SECURITY ASSESSMENTS ARE PERIODIC, NOT CONTINUOUS

Penetration tests and vulnerability scans are usually carried out periodically. However, the technology environment changes constantly.

Every day, the following can appear:
- New assets
- New configurations
- New integrations
- New identities

This means that an assessment carried out a few months ago may not reflect current exposure.

Key questions:
- How often do we assess our attack surface?
- Do we have continuous visibility into changes in the environment?

5. THERE IS NO VISIBILITY INTO POSSIBLE ATTACK PATHS

An isolated vulnerability may not represent a significant risk. But when several vulnerabilities combine, they can create an attack path that makes it possible to compromise critical systems.

For example:
External access ➔ compromised credential ➔ lateral movement ➔ access to sensitive information

Many organizations have no visibility into these potential attack paths.

Key questions:
- Can we identify how an attacker could move within our network?
- Do we understand which assets could be used as an entry point?

FINAL THOUGHT

If your organization identifies with several of these signs, its risk exposure is probably greater than currently perceived.

Modern security is not just about identifying vulnerabilities. It is about understanding how exposed the organization really is to a potential attack.