Boost AI Newsletter

MONTHLY BACKGROUND SERIES

Interreg North-West Europe
Co-funded by the European Union
Boost AI

Boost AI – Monthly Background Newsletter

October 2026 Edition

The AI Arms Race: Cybersecurity and the Business Race to Keep Up

When the Rules Change Overnight

Imagine your company website, booking system or customer portal suddenly needs an emergency security update. Do you know whether you are affected, how quickly you could respond - and what to do if the service must temporarily go offline?

That question became very real on 21 October 2026. Two critical vulnerabilities in PHP, the software behind many websites and online business applications, led to urgent patches and precautionary website shutdowns. They could allow attackers to run malicious code on vulnerable servers.

What makes this incident especially revealing is the role of Artificial Intelligence (AI). A weakness first noticed in 2024 was shown to be far more dangerous through AI-assisted research in 2026. Security researchers, including Calif, Wiz and OpenAI, worked with PHP maintainers and other partners to understand the threat and prepare protection.

The PHP crisis - at a glance

THE FLAW

Two critical PHP vulnerabilities (CVE-2026-109618 and CVE-2026-109619) were fixed in emergency releases on 21 October.

THE RESPONSE

Researchers and maintainers coordinated patches; hosting and security providers prepared additional defences.

THE IMPACT

Website operators worldwide had to assess exposure quickly, install updates or temporarily limit access.

This Is Bigger Than One Software Bug

PHP2Shell is a vivid example of a broader shift: AI can help people discover, analyse and respond to technical problems much faster. But the same progress also lowers the effort needed to develop offensive tools. For SMEs, that changes the speed of the challenge - not just its technical complexity.

The Security Arms Race - With AI on Both Sides

The familiar contest between computer viruses and antivirus software is entering a new phase. Defenders build better protection, attackers adapt, and defenders respond again. AI can make each round happen more quickly.

A faster cycle of discovery, attack and defence

1 DISCOVER	2 EXPLOIT	3 DEFEND
AI-assisted researchers inspect large codebases and test complex security weaknesses.	Adversaries can also use automation and AI to understand disclosures and develop attack tools faster.	Maintainers, hosting providers and IT teams patch, monitor, prioritise and validate protections.

The cycle does not stop at publication. Each new finding and countermeasure can trigger another round.

From Vulnerability to Attack in Hours

Once a security patch becomes public, it can also provide clues about the original flaw. AI-assisted researchers have demonstrated that a working PHP exploit can be reconstructed from the published fixes within hours. Separately, security teams observed attempts to exploit the vulnerabilities even before their public disclosure, followed by more activity after release.

This does not mean every attacker used AI. It does mean that the time between discovery, disclosure and potential exploitation is shrinking. Defenders cannot assume they have weeks to react to an urgent security warning.

The Old Virus-versus-Antivirus Analogy Still Fits

In the past, antivirus vendors recognised a threat, developed signatures and updates, and attackers looked for ways around them. Today, the same contest extends to software flaws, cloud services, identity systems and digital business processes. AI can support vulnerability research, security monitoring, incident analysis and documentation - while adversaries can use similar capabilities.

There is one essential difference from the headlines: strong protection still depends on basics such as keeping software updated, using supported systems, limiting access and testing backups. An AI assistant cannot compensate for an unpatched server.

What About Competition in Your Core Business?

The same acceleration is happening outside IT. AI-enabled competitors may answer customers faster, analyse information sooner, shorten development cycles or reduce routine administrative work. Even if you never build your own AI model, customers and partners may increasingly expect that level of speed.

Customer service

Faster answers and better service become the new benchmark when competitors automate routine requests.

Operations

AI-assisted forecasting, anomaly detection and document handling can shorten decision cycles.

Products and services

Teams can prototype, test and improve offerings more quickly - if they still verify quality.

Internal knowledge

Finding and summarising relevant information can make a small team more responsive.

The business risk is therefore not simply "using AI" versus "not using AI". It is whether your organisation can keep learning, evaluating tools and adapting processes as expectations change.

What SMEs Can Do Now - Without Becoming AI Experts

A useful response is not to rush into every new tool. It is to make your organisation faster at noticing change, deciding what matters and acting safely. These six steps combine sound security practice with practical AI adoption.

1 Know what you depend on

List critical websites, applications, suppliers, software versions and AI tools. Name the person responsible for each.

2 Make updates a fast process

Follow vendor advisories, prioritise internet-facing systems, and have a clear escalation path when an urgent patch appears.

3 Keep the fundamentals strong

Use supported software, prompt patching, access controls, multifactor authentication, monitoring and tested backups.

4 Use AI as a checked assistant

Summarise advisories, review inventories and logs, draft checklists, or compare mitigation options - but verify the results.

5 Experiment where value is measurable

Choose one concrete business use case, define time saved or quality gained, test with users and keep human approval.

6 Protect data and plan a fallback

Avoid sending secrets to unapproved services. Decide how work continues if an AI tool, cloud API or key supplier is unavailable.

A useful 20-minute exercise

Ask two questions: Which business-critical website or process would hurt us most if it stopped tomorrow - and who would respond? Which routine task or customer expectation could change significantly if AI made it faster or cheaper?

AI Helps - But It Does Not Replace Responsibility

AI can help with research, explanations and draft plans, but important claims and technical changes require verification. Keep personal data and trade secrets out of unapproved services. Human expertise and accountability remain essential.

Looking Forward

The lesson from PHP2Shell is not that every SME needs its own cybersecurity AI. It is that the pace of technological change is increasing for defenders, attackers and competitors alike. Companies that combine reliable fundamentals with curious, structured AI experimentation will be better placed to adapt.

Content provided by the Machine Learning Group at RPTU for the Boost AI Monthly Background Newsletter series, October 2026 edition.

Steffen Reithermann <steffen.reithermann@cs.rptu.de> - ml.cs.rptu.de

Newsletter archive: ml.cs.rptu.de/projects/Boost-AI/newsletter/

RPTU Rheinland-Pfälzische Technische Universität Kaiserslautern Landau