Jak zajistit, aby vaše IT prostředí bylo schopné zpětně vyhodnotit, analyzovat a právně obhájit jakýkoliv bezpečnostní incident – bez ohledu na velikost firmy.

V době, kdy je e-mail hlavním nástrojem komunikace a zároveň běžným cílem kybernetických útoků, nestačí jen „fungovat“. Je třeba umět **dokázat**, že infrastruktura byla spravována bezpečně, že byla schopná incident včas identifikovat – a že lze zpětně rekonstruovat jeho průběh.
Malé a střední podniky (SME) často nemají vlastní bezpečnostní tým, přesto mohou být dobře připravené – díky otevřeným standardům, chytrému nastavení a přiměřené dokumentaci.

Klíčové pilíře forenzní připravenosti

Oblast	Co znamená v praxi
Auditní stopy	Uchovávání logů, přístupových záznamů, e-mailových tras
Retenční politika	Jasné pravidlo, jak dlouho se ukládají data (např. logy 90 dní)
Zabezpečení schránek	Ochrana hesel, 2FA, izolace kritických rolí
Reprodukce incidentu	Možnost zpětně analyzovat, co se stalo (čas, IP, uživatel, soubor)
Soulad s právem	Dodržování GDPR, archivace dat a auditovatelnost procesů
Školení a procesy	Správce ví, co dělat, když dojde k podezřelé aktivitě

📋 Checklist forenzní připravenosti (pro správce e-mailového systému)

✅ Logy přístupů na IMAP/SMTP uchovávám alespoň 90 dní

✅ E-mailová relace (MAIL FROM / RCPT TO / relay IP) se ukládá do syslogu nebo **SIEM*** (Security Information and Event Management – systém pro sběr a analýzu logů) (viz. níže)

✅ Mám detekci neobvyklého chování (např. přihlášení z cizího regionu)

✅ Antispamový systém (Rspamd) loguje score a rozhodnutí v detailu

✅ Webmail (např. SOGo) má audit zapnutí/offline režimu, exportu kontaktů apod.

✅ Všechny přístupy přes web UI mají logovací mechanismus a TLS enforcement

✅ Zálohování VM obsahuje metadata i logy, není rotováno bez validace

✅ Uživatelé nemohou měnit SPF/DKIM bez administrátorského přístupu

✅ Existuje směrnice pro práci s e-mailovou schránkou při odchodu zaměstnance

✅ V případě incidentu mám dokument, jak vytáhnout logy, přehled schránek a přístupy
„Pro sběr logů z e-mailového serveru lze využít open-source nástroje jako Wazuh, Graylog nebo OSSEC, které umožňují sledovat relace, přihlašování i anomálie.“ (viz. níže)

🎓 Doporučení pro malé firmy

- I bez SIEM nebo externího auditního systému lze dosáhnout vysoké úrovně bezpečnosti – stačí mít logiku, smysl pro konzistenci a pravidelně ověřovat funkčnost
- Dokumentace může mít podobu **textového souboru v Git repozitáři, nebo PDF s verzováním** – nepotřebujete systém za miliony
- Forenzní připravenost není paranoia – je to **právní štít**, když někdo zneužije firemní e-mail, napadne server nebo exfiltruje kontakty

---

*SIEM je zkratka pro **Security Information and Event Management** — v češtině by se to dalo přeložit jako „**Správa bezpečnostních informací a událostí“**.

🧠 Co SIEM vlastně dělá?

Je to systém, který:

- **Sbírá logy a události** ze všech zařízení v síti (firewally, servery, e-mailové systémy, webmail, VPN…)
- **Analyzuje je v reálném čase** → hledá podezřelé chování, útoky, anomálie
- **Umožňuje zpětně rekonstruovat incident** → kdo, kdy, odkud, co udělal
- **Pomáhá s compliance** → GDPR, ISO 27001, NIS2, HIPAA, PCI-DSS…

🔍 Příklad z praxe:

Když se někdo přihlásí do webmailu z Ruska ve 3 ráno, SIEM to:

1. **Zaznamená** jako událost
2. **Porovná s běžným chováním uživatele**
3. **Vyhodnotí jako anomálii**
4. **Pošle alert správci**
5. **Umožní dohledat celý průběh** (IP, čas, akce, přístup k souborům…)

📦 Co SIEM není?

- Není to firewall, ale **nadstavba nad logy**
- Není to antivir, ale **centrální mozek pro bezpečnostní analýzu**
- Není to jen logovací systém — umí **korelaci, alerty, reporting**

🧠 Top open-source SIEM nástroje vhodné k mailserveru

🛠️ Nástroj	Co umí / Proč se hodí k mailserveru	Poznámka k nasazení
Wazuh	HIDS + SIEM: logy, integrity check, rootkit detekce, compliance	✅ Docker / VM / bare-metal
OSSEC	Host-based IDS, logy z mailserveru, detekce změn	✅ Lehký, ale méně UI-friendly
Security Onion	Kompletní distro: Suricata, Zeek, ELK, Wazuh, Kibana	⚠️ Náročnější na HW, ale komplexní
Graylog	Log management + alerty, vizualizace, geolokace IP	✅ Moderní UI, vhodné pro SMTP/IMAP logy
ELK Stack	Elasticsearch + Logstash + Kibana → logy, dashboardy	⚠️ Nutná konfigurace korelace
Snort / Suricata	IDS/IPS pro síťovou vrstvu, SMTP traffic, port scan	✅ Doplněk k SIEM, ne SIEM samotný
Prelude SIEM	Korelace událostí, IDMEF standard, integrace s OSSEC/Snort	⚠️ Méně známý, ale standardizovaný
MozDef	SIEM od Mozilly, microservices, alerty, Elastic backend	⚠️ Vyžaduje čas na nastavení

🔐 Co sledovat u mailserveru pomocí SIEM

- **SMTP relace**: MAIL FROM / RCPT TO / relay IP
- **IMAP/POP3 přihlášení**: čas, IP, geolokace, počet pokusů
- **Webmail akce**: export kontaktů, přístup z mobilu, offline režim
- **Antispam rozhodnutí**: score, reject důvody, greylisting
- **TLS handshake**: verze, cipher, expirace certifikátu
- **DKIM/SPF/DMARC logy**: validace, selhání, spoofing pokusy

💡 Doporučení

- Pro **lehké nasazení** k mailcow: **Wazuh** nebo **Graylog**
- Pro **komplexní monitoring**: **Security Onion** nebo **ELK Stack**
- Pro **síťovou vrstvu**: doplňit o **Suricata** nebo **Snort**
- Pro **forenzní audit**: kombinuj s logy z Postfixu, Dovecotu, rspamd
  Pokud si vše jmenované zvládnete sami nainstalovat a hlavně zkonfigurovat, máte TOP řešení kompletně zdarma, přičemž jeho reálná hodnota bude od stovek tisíc do několika milionů podle zvolené konfigurace v porovnání s komerčnímy systémy používanými například v bankovním sektoru.
  „Tento text není právní analýzou, ale technickým přehledem možností, jak podpořit bezpečnostní auditovatelnost e-mailového prostředí. V případě regulovaných odvětví doporučujeme konzultaci s právníkem.“
