DORA v praxi pre CASP

Peter Hidasy

26.3.2026

Licenčné konanie vs. onsite dohľad

- Súlad s nariadeniami
- Splnenie licenčných podmienok
- Prevažne teoretický pohľad

VS.

- Preverovanie v praxi
- Fyzický prístup do systémov
- Rámcové preverenie zmlúv

Dotazník

Oblasť	Číslo	Kontrolná otázka
Riadenie rizík a správa aktív	1	Používa vaša organizácia štandardizovaný prístup alebo rámec analýzy rizík na identifikáciu, klasifikáciu a dokumentáciu obchodných funkcií, informačných a IKT aktív a ich vzájomných závislostí (napr. ISO/IEC 27005, NIST SP 800-30, FAIR, OCTAVE, EBIOS Risk Manager, CRAMM alebo iný formalizovaný rámec v súlade s osvedčenými postupmi IKT riadenia rizík)?
	2	Používate softvérové nástroje na evidenciu a klasifikáciu IKT aktív a systémov podľa ich obchodného významu a rizika (napr. CMDB, asset inventory, cloud asset inventory nástroje)?
	3	Využívate automatizované riešenia na scoring a hodnotenie IKT rizík (napr. risk heatmap, dashboardy, GRC nástroje)?
	4	Využívate vo svojich procesoch alebo IT riešeniach (napr. GRC systéme) štandard OSCAL (Open Security Controls Assessment Language), resp. podporujú tieto riešenia jeho integráciu a prácu s ním?
	5	Využívate metriky a KPI/KRI na meranie výkonnosti a efektívnosti systému riadenia rizík IKT (napr. počet neakceptovaných rizík, doba uzavretia rizík)?
Kryptografia a šifrovanie	6	Zabezpečujete šifrovanie všetkých citlivých údajov v pokoji (na diskoch, databázach a zálohách) pomocou silných algoritmov (napr. AES)?
	7	Šifrujete sieťovú prevádzku na interných spojeniach (napr. medzi servermi, VM, kontajnermi)?
	8	Používate softvérový nástroj na správu životného cyklu šifrovacích kľúčov (generovanie, rotácia, zneplatnenie a zálohovanie)?
	9	Využívate vo svojich IT riešeniach alebo procesoch post-kvantové šifrovanie?
	10	Používate pri návrhu šifrovacích riešení štandardy a techniky podľa noriem (napr. NIST, ISO/IEC 19790, ENISA, ETSI, FIPS 140-3)?
	11	Využívate hardvérové kľúče vydané dôveryhodnou certifikačnou autoritou?
	12	Používate internú alebo externú PKI na overovanie používateľov alebo systémov?
Politiky a postupy v prípade operácií IKT	13	Používate automatizované nástroje na bezpečnú inštaláciu a správu konfigurácií?
	14	Používate automatizované nástroje pre zálohovanie?
	15	Prevádzkujete testovacie prostredie pre všetky kritické IKT systémy?
	16	Sú produkčné systémy prevádzkované v oddelenom prostredí od testovacích (min. oddelené databázy a úložiská dát, rozdielne účty a prístupové role pre produkciu a testovanie, samostatné servery alebo virtuálne prostredia)?
Riadenie kapacit a vykonu	17	Máte zavedené nástroje na sledovanie a notifikáciu pri hraničnom vyťažení systémových zdrojov (napr. CPU, RAM, disk, sieť)?
	18	Používate automatizované nástroje na optimalizáciu využívania výpočtových, sieťových a pamäťových kapacít (napr. load balancing, virtualizácia, autoscaling)?
	19	Realizujete pravidelné testovanie výkonnosti a záťažové testy?
	20	Sú IKT systémy s vysokou záťažou (napr. systémy spracúvajúce veľké objemy dát alebo transakcií) identifikované a špeciálne monitorované?
Riadenie zraniteľnosti a bezpečnostných záplat	21	Získavate priebežne informácie o relevantných zraniteľnostiach z dôveryhodných zdrojov (napr. CVE databáza)?
	22	Vykonávate automatizované skenovanie zraniteľností v kritických IKT systémoch aspoň raz týždenne?
	23	Monitorujete používanie knižníc tretích strán vrátane open source pomocou automatizovaných nástrojov (napr. OWASP Dependency-Check)?
	24	Vykonávate testovanie bezpečnostných záplat pred ich nasadením (napr. v staging/testovacom prostredí)?
	25	Využívate nástroje na automatické nasadzovanie bezpečnostných záplat v rámci vývojových prostredí, knižníc a závislostí softvéru?
	26	Využívate nástroje na automatickú inštaláciu bezpečnostných záplat pre operačné systémy a infraštruktúrne komponenty?
	27	Máte stanovené lehoty na aplikáciu záplat podľa úrovne rizika a závažnosti zraniteľnosti (napr. CVSS skóre)?
	28	Používate softvérový nastroj na evidenciu všetkých známych zraniteľností v IKT systémoch a sleduje sa ich riešenie?


Oblasti dohľadu

Úschova kryptoaktív

- Fyzická kontrola úschovy
- Kontrola zmlúv o úschove
- Živá ukážka podpisových politík
- Overenie fyzickej distribúcie kľúčov
- Segregácia prostriedkov

Monitorovanie incidentov

- Živá ukážka monitorovania
- Ukážka SOC/SIEM
- Kontrola logov

Riziká výpadku dodávateľov

- Záložní dodávatelia
- Kontrola exit stratégií
- RTO test – migrácia na záložného dodávateľa

Aktualizovaná dokumentácia

- Plán kontinuity činnosti
- Disaster recovery plan
- Riziková analýza
- Retesty

Špecifiká biznis modelov

- Dôraz na fyzickú bezpečnosť pri kryptomatoch
- Odolnosť oracles v smart kontraktoch
- Double spending pri kupónoch
- Postupy onchain monitoringu
- ...

- V prípade potreby si prizveme dodávateľov

Otázky

NÁRODNÁ BANKA SLOVENSKA
EUROSYSTÉM

NBS je aj

Múzeum mincí a medailí v Kremnici
5peňazí
Nadácia NBS
Inštitút bankového vzdelávania