Deloitte.

SWIFT Customer Security Programme

Řízení rizik společnosti Deloitte

Rámec a použitelnost

Rámec nazvaný Customer Security Controls Framework představuje soubor základních bezpečnostních kontrol, které jsou pro **uživatele systému SWIFT povinné**. Účelem těchto kontrol je pomoci **zmírnit specifická kybernetická bezpečnostní rizika**, jimž uživatelé systému SWIFT čelí v prostředí, kde existují kybernetické hrozby. Příkladem mohou být neoprávněné realizace nebo modifikace finančních transakcí, zpracování pozměněných či neoprávněných zpráv SWIFT apod

SWIFT Customer Security Controls Framework

Objectives	Staregic Security Principles
01. Secure Your Environment	P1. Restrict Internet access and Protect critical systems from general IT environment
	P2. Reduce attack surface & vulnerabilities
	P3. Physically secure the environment
02. Know and Limit Access	P4. Prevent compromise of credentials
	P5. Manage identities & segregate privileges
03. Detect and Respond	P6. Detect anomalous activity to system or transaction records
	P7. Plan for incident response

2021

Co přináší rok 2021

Vlastní ověřování na základě posouzení standardů společenství SWIFT je od roku 2021 **povinné**.

Co je tzv. community-standard assessment?

Community-standard assessment je posouzení prováděné **nezávislou třetí stranou** (např. Deloitte) nebo vaší druhou či třetí úrovní obrany, např. interním oddělením compliance, řízení rizik nebo oddělením interního auditu (které jsou nezávislé na první linii obrany, která vlastní ověření předkládá).

Klíčové činnosti pro splnění milníků CSP v roce 2021 a dalších letech

2020

Vydání CSCF v2020

- 2 kontroly prohlášeny za povinné a přidány 2 doporučené kontroly, 1 rozšíření rozsahu kontrol
- Sladění kontrol s realitou s možností alternativních implementací.
- Vyjasnění stávajících kontrol.

Kvůli onemocnění covid-19 byli uživatelé oprávnění provádět vlastní ověřování dle CSCFv2019 do 31.12.2020. Community-standard assessment je povinné až od roku 2021.

2021

Vydání CSCF v2021
Community-standard assessment je povinné.

- Nový typ architektury A4, která umožňuje uživatelům s middleware serverem nezavádět bezpečnou zónu (kontrola 1.1).
- Vysvětleny stávající kontroly a požadavky na architekturu.
- Přístup založený na riziku pro plnění kontrolních cílů.
- Při přístupu ke službě související se systémem SWIFT provozované třetí stranou se očekává použití multifaktorové autentizace.

31 kontrol v roce 2021

Zaveden nový typ architektury A4	**Vlastní ověření do 31.12.2021**	**1 kontrola povýšena na povinnou**	**1 kontrola prohlášena za povinnou**	**Aktualizace definice konektoru**

Jedinečné odborné předpoklady pro oblast Customer Security Controls Framework (CSCF) (rámec používaný pro SWIFT CSP)

V rámci tohoto programu společnost Deloitte dosud provedla po celém světě více než 100 posouzení na základě SWIFT CSCF.

Centrum excelence společnosti Deloitte pro SWIFT CSP

Abychom ve všech regionech poskytovali služby prvotřídní kvality a vycházeli z vlastních zkušeností, vytvořila společnost Deloitte centrum excelence pro SWIFT CSP sdružující odborníky, kteří mají dovednosti a zkušenosti s projekty zajištění bezpečnosti na základě SWIFT Customer Security Controls Framework (CSCF). Naši odborníci projekty realizovali od začátku do konce nebo podporovali místní pobočku Deloitte při posuzování bezpečnosti na základě CSCF jako odborníci na danou problematiku.

Metodologie sestavená pro potřeby SWIFT CSP

Společnost Deloitte má ukázkové výsledky při posuzování provozních a bezpečnostních rizik na základě SWIFT CSCF.
S využitím vlastních zkušeností jsme vytvořili přesně uzpůsobenou metodologii na základě SWIFT CSCF a mezinárodních bezpečnostních standardů specifických pro tento typ zakázek.

66 *Ve společnosti Deloitte máme jedinečnou pozici a odborné předpoklady, díky nimž můžeme vaší organizaci předložit bezprecedentní pohled na vaši SWIFT infrastrukturu. Naši odborníci na tuto problematiku vám rádi poskytnou další informace.*

Kontakty

Jakub Höll
Manažer
+420 734 353 815
jholl@deloittece.com

Jakub Ponec
Senior Konzultant
+420 773 768 762
jponec@deloittece.com