TelekomSlovenije

OPERATIVNI CENTER **KIBERNETSKE VARNOSTI**

Bodite pripravljeni na kibernetske grožnje.

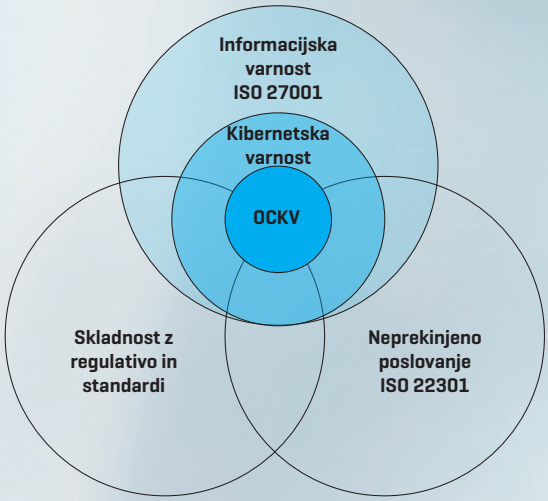
Podjetja in organizacije se vse bolj zavedajo kibernetskih groženj in varnostnih tveganj, ki jih prinašajo sodobno, odprto in informacijsko vsepovezano poslovanje ter digitalizirani procesi upravljanja sistemov in infrastrukture. Tveganja izhajajo na eni strani iz ranljivosti sistemov ter na drugi strani iz akterjev, ki te ranljivosti zlorabljajo in so vse bolj usposobljeni. Zato se danes kibernetska varnostna tveganja že uvrščajo med najpomembnejša operativna tveganja.

Strokovnjaki v Operativnem centru kibernetske varnosti Telekoma Slovenije vam pomagajo tovrstna tveganja obvladovati. Operativni center kibernetske varnosti je certificiran po mednarodnem standardu za informacijsko varnost ISO 27001, ob tem pa ima Telekom Slovenije tudi certifikat za neprekinjeno poslovanje ISO 22301.

www.telekom.si/poslovni

Dolgoročna varnost podjetij in organizacij z vidika operativnih tveganj temelji na obvladovanju regulatornih zahtev, na skladnosti in neprekinjenosti poslovanja ter na informacijski in kibernetski varnosti.

Zaradi vedno večje kompleksnosti kibernetskih varnostnih groženj **operativni center kibernetske varnosti postaja nuja** in je postavljen v središče kibernetske varnosti.



Hitro odzivanje na dogodke in njihovo reševanje na različnih nivojih, organiziranje ob kriznih situacijah ter ustrezno poročanje je le nekaj dejavnikov, ki jih v Telekomu Slovenije skrbno načrtujemo. Svoje izkušnje smo iz obstoječih operativnih služb omrežnega operativnega centra NOC (Network Operations Center) in storitvenega operativnega centra SOC (Service Operations Center) prenesli tudi v Operativni center kibernetske varnosti (OCKV).

Operativni center kibernetske varnosti Telekoma Slovenije ima vgrajene vse ključne elemente, ki zagotavljajo **učinkovito operativno delovanje**: preizkušene **procese**, vrhunsko **tehnologijo**, izkušene **strokovnjake** ter **zanesljive vire** kibernetskih varnostnih informacij.

Pomemben člen v procesu je tudi ustrezna storitvena podpora, kjer vodimo incidente in skrbimo za njihovo reševanje skladno z dogovorom o ravni storitev (Service Level Agreement - SLA).

Z operativnim centrom kibernetske varnosti naročnikom zagotavljamo:

- **hitro in učinkovito odzivanje** na kibernetske napade,
- **omejitev in zmanjševanje škode** ob morebitnem kibernetskem napadu,
- **zbiranje in zavarovanje dokazov,**
- **zvišanje odpornosti** in **znižanje kibernetskih varnostnih tveganj,**
- **zajem in hramba dogodkov**, zagotavljanje revizijskih sledi,
- **seznanjenost naročnika** s pomembnimi dogajanji in predlogi ukrepov,
- **doseganje skladnosti** npr. z Zakonom o informacijski varnosti, GDPR, ISO-standardi.

Uvedba kibernetske varnostne operative je kompleksen in dolgotrajen proces, ki lahko podjetjem oz. organizacijam brez ustrezne kadrovske in finančne podpore predstavlja težko premostljiv izziv. V Telekomu Slovenije za vsako podjetje poiščemo ustrezne rešitve kibernetske varnosti, k uvedbi pa pristopamo projektno.

Celotni proces kibernetske varnostne operative temelji na zajemu relevantnih dogodkov z vidika informacijske varnosti iz najrazličnejših sistemov pri naročnikih ter lokalnega in globalnega okolja. Incidenti se rešujejo po spodaj predstavljenem paketu. Po potrebi v reševanje vključimo ustrezne druge službe in državne organe v okviru veljavnih predpisov in sklenjenih dogovorov.

V Telekomu Slovenije skladno z dogovorom z naročnikom izvajamo **aktivno zaščito, preprečujemo napade onemogočanja DDoS,** varujemo pred **dostopom do škodljivih spletnih vsebin** in izvajamo **druge tehnične ukrepe** na lokaciji naročnika ali Telekoma Slovenije.

Potek izvajanja storitve Operativnega centra kibernetske varnosti

Za več informacij:

- pokličite **svojega osebnega svetovalca**,
- pišite na **poslovna.prodaja@telekom.si**,
- obiščite **www.telekom.si/poslovni**.

Za morebitne tiskarske napake se opravičujemo. Slika je simbolična.

Telekom Slovenije, d.d., Ljubljana
TL 4.1.4/91.1 (20. 6. 2018)