WISER

Wide-Impact cyber SEcurity Risk framework

Direktiva NIS o varnosti omrežij in informacij – vodič in pogosta vprašanja

www.cyberwiser.eu | info@cyberwiser.eu | @cyberwiser

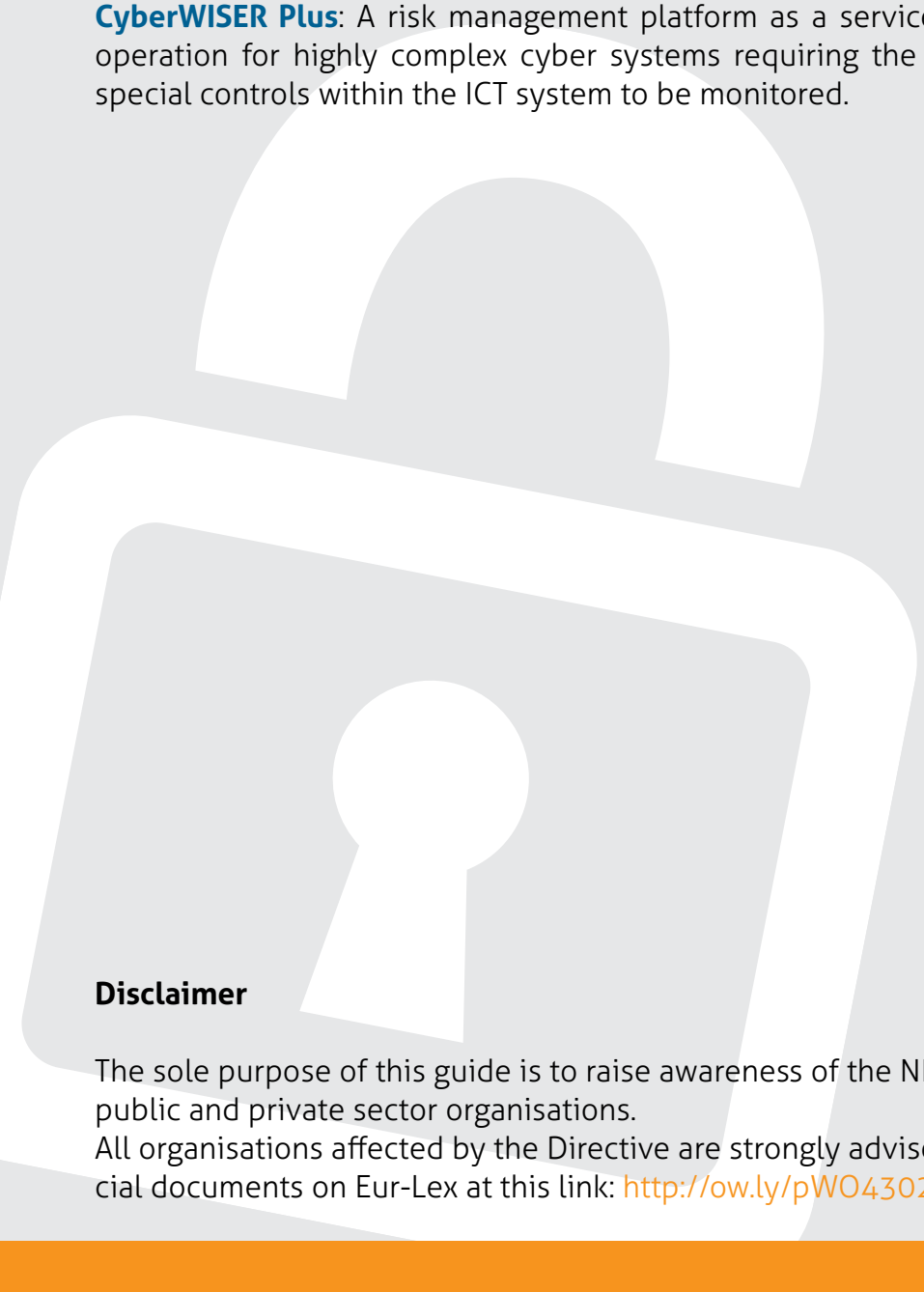
WISER is an Innovation Action funded under the Horizon 2020 programme, developing a cyber-risk management framework to assess, monitor and mitigate risks. WISER is rolling out a suite of smart services for ICT-intensive SMEs and owners complex ICT systems and critical infrastructures across multiple industries.

CyberWISER Light is a free, online service comprising a questionnaire that gives you a downloadable, personalised cyber risk profile and a vulnerability test to help you prevent attacks with a downloadable customised report.

New services coming in late 2016:

CyberWISER Essential: a pre-packaged risk management solution for SMEs.

CyberWISER Plus: A risk management platform as a service (RMaaS) mode of operation for highly complex cyber systems requiring the implementation of special controls within the ICT system to be monitored.



Disclaimer

The sole purpose of this guide is to raise awareness of the NIS Directive for public and private sector organisations.
All organisations affected by the Directive are strongly advised to read the official documents on Eur-Lex at this link: http://ow.ly/pWO4302Gs10

Direktiva NIS za varnost omrežij in informacij – vodič in pogosta vprašanja

Direktiva za varnost omrežij in informacij (NIS – Network and Information Security) je poenotila uredbe o kibernetski varnosti na nivoju celotne Evropske Unije.

Veljati je začela **avgusta 2016**. Države članice imajo za izvajanje Direktive in vpeljevanje v nacionalno zakonodajo na voljo 21 mesecev in 5 dodatnih mesecev za identifikacijo administratorjev kritične infrastrukture.

Direktiva želi zagotoviti visoko raven varnosti omrežij in informacij v EU. Cilji Direktive so naslednji:

» krepitev obrambnih kibernetskih zmogljivosti na nacionalni ravni;
» krepitev kibernetske varnosti EU z mednarodnim sodelovanjem;
» uvedba obveznega upravljanja s tveganji in poročanja o incidentih za administratorje kritične infrastrukture in ponudnike digitalnih storitev

1. Ukrepi držav članic za krepitev obrambnih kibernetskih zmogljivosti na nacionalni ravni

Vsaka država članica bo sprejela nacionalno strategijo za varnost omrežij in informacijskih sistemov in ustrezno določila strateške cilje in regulativne ukrepe. Ključne točke strategije:

» strateški cilji, prednostne naloge in model upravljanja;
» določitev meril za ustrezno stopnjo pripravljenosti, odzivnosti in zmogljivosti za ponovno vzpostavitev stanja po incidentu;
» sodelovanje javnega in zasebnega sektorja;
» izvajanje programov ozaveščanja in uvedba vsebin s področja kibernetske varnosti za izobraževanje in usposabljanje;
» okvirni program za raziskave in razvoj izvajanja strategije NIS za varnost omrežij in informacij;

» okvirni program za oceno in upravljanje s tveganji;
» seznam ključnih akterjev za izvajanje strategije.

Države članice bodo določile enega ali več pristojnih kompetentnih organov za nadzor in implementacijo Direktive NIS na nacionalni ravni.

Države članice bodo določile enotno kontaktno točko za komunikacijo in sodelovanje z relevantnimi organi v drugih državah članicah.

Države članice bodo imenovale enega ali več **nacionalnih odzivnih centrov CSIRT**, ki so odgovorni za (vključno z, vendar ne omejeno na):

» nadzor in spremljanje incidentov na nacionalni ravni;
» zagotavljanje zgodnjega odkrivanja, vzpostavitev učinkovitega sistema obveščanja ter razširjanje informacij o tveganjih in incidentih med ključnimi skupinami;
» odziv na incidente;
» dinamična analiza, ocena tveganj, možnosti incidentov in stopnja ozaveščenosti o kibernetski izpostavljenosti;
» sodelovanje v mreži nacionalnih odzivnih centrov CSIRT.

2. Ukrepi držav članic za krepitev kibernetske varnosti EU z mednarodnim sodelovanjem

Direktiva NIS določa oblikovanje **Kooperativne skupine** za podporo sodelovanju na strateški ravni, izmenjavo informacij med državami članicami, in vzpostavitev medsebojnega zaupanja.

Direktiva določa tudi vzpostavitev mreže nacionalnih odzivnih centrov za zagotavljanje pogojev medsebojnega zaupanja med državami članicami in za spodbujanje hitre komunikacije ter učinkovitega sodelovanja na operativni ravni.

Katere so naloge Kooperativne skupine?

Kooperativno skupino sestavljajo predstavniki držav članic, Komisija in ENISA (The European Union Agency for Network and Information Security), Evropska Komisija sodeluje v vlogi sekretariata.

Delovanje Kooperativne skupine temelji na dvoletnem delovnem programu s tremi stebri:

Načrtovanje:

» oblikovanje Delovnega programa 18 mesecev po začetku veljavnosti (npr. februar 2018);

» oblikovanje delovnega programa vsaki naslednji dve leti

Usmerjanje:

» pomoč, zastavljene smernice mreži odzivnih centrov CSIRT;

» pomoč in podpora državam članicam pri krepitvi nacionalne omrežne in informacijske varnosti;

» podpora državam članicam pri identifikaciji kritične infrastrukture in storitev;

» najboljše prakse sistema za obveščanje in notifikacij;

» standardizacija in razprave povezane z njo;

» povezovanje s ključnimi institucijami in organizacijami EU;

» evalvacija nacionalnih strategij NIS in mreže odzivnih centrov CSIRT (na prostovoljni osnovi);

» izmenjava informacij in najboljših praks s področja:

  » tveganj,

  » incidentov,

  » osveščanja,

  » usposabljanja,

  » R&R (raziskave in razvoj).

Poročanje:

Vsaki dve leti bo skupina pripravila poročilo o s sodelovanjem pridobljenih izkušnjah. Poročilo bo poslano Evropski Komisiji kot del evalvacije delovanja Direktive.

Katere so naloge mreže CSIRT?

Mrežo CSIRT sestavljajo predstavniki držav članic, centrov za odzivanje na varnostne incidente CSIRT in CERT-EU (the Computer Emergency Response Team for the EU institutions, agencies and bodies). Komisija sodeluje v mreži CSIRT kot opazovalec. ENISA sodeluje v vlogi sekretariata in podpore sodelovanju med odzivnimi centri CSIRT.

Mreža CSIRT izvaja naslednje naloge:

» izmenjava informacij o kapacitetah odzivnih centrov, dejavnostih in možnostih sodelovanja;

» izmenjava informacij o incidentih (na zahtevo in na prostovoljni osnovi);

» prepoznavanje situacij, ki zahtevajo koordiniran odziv na incidente (na zahtevo in na prostovoljni osnovi);
» podpora čezmejnemu obravnavanju incidentov (na prostovoljni osnovi);
» iskanje novih oblik sodelovanja na operativni ravni;
» obveščanje Kooperative skupine o aktivnostih in zahtevki za smernice o nadaljnjih postopkih;
» možnost razprave o znanju in izkušnjah pridobljenih v okviru usposabljanj NIS;
» možnost razprave s posameznimi odzivnimi centri (na zahtevo);
» objava smernic za sodelovanje na operativni ravni.

Dve leti po začetku veljave Direktive NIS in nato vsakih 18 mesecev bo mreža CSIRT pripravila poročilo o izkušnjah, pridobljenih na operativni ravni, katere del bo tudi ocena in priporočila. Poročilo bo poslano Komisiji kot pregled nad delovanjem Direktive.

Upravljanje s tveganji in obveščanje o incidentih – obveznosti administratorjev kritične infrastrukture in ponudnikov digitalnih storitev.

Kdo so administratorji kritične infrastrukture in kakšne so njihove naloge?

Administratorji kritične infrastrukture so zasebna podjetja ali pravne osebe, katerih dejavnost ima pomemben vpliv na družbo in gospodarstvo.

Identificirani administratorji kritične infrastrukture bodo morali v sklopu Direktive NIS podvzeti ustrezne varnostne ukrepe in obveščati pristojne organe o incidentih.

Varnostni ukrepi vključujejo:

» obvladovanje tveganj: ustrezni ukrepi na tehnični in organizacijski ravni;
» zagotavljanje varnosti omrežij in varnostnih sistemov: ukrepi morajo zagotoviti ustrezen nivo varnosti;
» odziv in ravnanje ob incidentih: ukrepi morajo zagotoviti nemoteno delovanje računalniških sistemov in minimalizirati posledice v primeru incidenta.

Kako identificirati administratorje kritične infrastrukture?

Vsaka država članica bo določila subjekte, ki bodo morali podvzeti ustrezne varnostne ukrepe in poročati o incidentih pristojnim organom po naslednjih kriterijih:

(1) Subjekt je ponudnik storitev, ki so ključnega pomena za vzdrževanje in nemoteno delovanje gospodarskih in družbenih dejavnosti.

(2) Nemoteno delovanje storitev ponudnika je odvisno od delovanja omrežja in informacijskih sistemov.

(3) Varnostni incident bi prekinil ali resno okrnil delovanje storitev.

Katere sektorje zajema Direktiva?

Direktiva zajema naslednje sektorje:

» energija: elektrika, nafta, plin;
» transport: letalski, železniški, vodni, cestni;
» bančništvo: kreditne institucije;
» finančni trgi: mesta trgovanja, centralne nasprotne stranke;
» zdravje: zdravstvene ustanove;
» voda: dobava in distribucija pitne vode;
» digitalna infrastruktura: internetne izmenjevalne točke, ponudniki domen (DNS), registri domen najvišje ravni (TLD).

O katerih incidentih naj bi poročali administratorji?

V Direktivi ni strogo določeno, o katerih incidentih naj bi poročali administratorji. Pri določanju stopnje resnosti incidenta naj bi upoštevali naslednje 3 parametre:

» št. prizadetih uporabnikov,
» trajanje incidenta,
» geografska razširjenost oz. doseg.

Ti parametri bodo dodatno pojasnjeni s smernicami, ki jih sprejmejo pristojni nacionalni organi in Kooperativna skupina.

Kdo so ponudniki digitalnih storitev (DSP – Digital Service Providers), in katere bodo njihove naloge?

Ponudniki digitalnih storitev (DSP) bodo morali podvzeti ustrezne ukrepe, in o incidentih obveščati pristojne organe.

Varnostni ukrepi zajemajo:

» obvladovanje tveganj: ustrezni ukrepi na tehnični in organizacijski ravni;
» zagotavljanje varnosti omrežij in varnostnih sistemov: ukrepi morajo zagotoviti ustrezen nivo varnosti;
» odziv in ravnanje ob incidentih: ukrepi morajo zagotoviti nemoteno delovanje računalniških sistemov in minimalizirati posledice v primeru incidenta.

Ponudniki digitalnih storitev (DSP) bodo morali upoštevati tudi naslednje dejavnike, ki jih bo natančneje opredelila Komisija z izvedbenim aktom:

» varnost sistemov, strojne opreme, naprav;
» odziv in ustrezno ravnanje ob incidentih;
» zagotavljanje pogojev za neprekinjeno poslovanje;
» spremljanje, revizija, testiranje;
» skladnost z mednarodnimi standardi.

O katerih incidentih naj bi poročali ponudniki digitalnih storitev (DSP)?

V Direktivi ni strogo določeno, o katerih incidentih naj bi poročali. Pri določanju stopnje resnosti incidenta naj bi upoštevali 5 parametrov:

» št. prizadetih uporabnikov;
» trajanje incidenta;
» geografska razširjenost, doseg;
» stopnja okrnitve oz. prekinitve zagotavljanje storitve;
» posledice za gospodarske in družbene dejavnosti.

Ti parametri bodo dodatno pojasnjeni z izvedbenimi akti, ki jih sprejme Komisija.

Kateri ponudniki digitalnih storitev so zajeti?

» spletni trg, ki omogoča podjetjem, da ponujajo svoje produkte in storitve na enem mestu;
» storitve oblačnega računalništva;

» iskalniki.

Za vse subjekte, ki ustrezajo opredelitvam, samodejno veljajo varnostne zahteve in obveznost priglasitve v skladu z Direktivo NIS. Mikro in mala podjetja niso zajeta v Direktivi (kot je opredeljeno v priporočilu Komisije 2003/361/EC).

Kako doseči usklajen a prožen pristop za ponudnike digitalnih storitev (DSP)?

Komisija bo sprejela izvedbene akte o varnostnih zahtevah in obveznosti priglasitve za DSP v roku enega leta od sprejetja te Direktive. Države članice ne bodo mogle dodatno zaostriti zahtev po varnosti in obveznosti priglasitve za DSP. Poleg tega bodo pristojni organi lahko opravljali nadzor le v primeru dokaza, da DSP ni izpolnjeval svojih obveznosti, kot so določeni v Direktivi.

Povezave:

Network and Information Security (NIS) Directive

http://ow.ly/pWO4302Gs10

Digital Single Market: cyber security http://ow.ly/Pc9I302Gs5A

Fact Sheet on Cyber Security in EU http://ow.ly/YkSJ302Gs83

EC Press Release on NIS Directive approval by EU Parliament http://ow.ly/Z5Nk302Gsaf

Strategija kibernetske varnosti – ENISA (Evropska agencija za varnost omrežij in informacij) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/si-ncss

EU enotno k zaščiti interneta
https://www.cert.si/eu-enotno-k-zasciti-interneta/

Strategija kibernetske varnosti Digitalna Slovenija http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/pdf/Digitalna_Slovenija_2020_29_8_14_Strategija_kib_varnost1.pdf

What is the timeline for implementation of the Directive?

AON Atos ENERVALIS Rexel a world of energy

SINTEF Trust-IT Trust-IT Services Ltd Communicating ICT to markets XLAB NOT IDLE

Join WISER for free access to CyberWISER Light and support, updates and key insights

Sign-up for our newsletter:

Follow us on twitter:

Connect on LinkedIn:

European Commission