IL-KUMMISSJONI
EWROPEA

Brussell, 15.1.2025
COM(2025) 10 final

KOMUNIKAZZJONI TAL-KUMMISSJONI LILL-PARLAMENT EWROPEW, LILL-KUNSILL, LILL-KUMITAT EKONOMIKU U SOĊJALI EWROPEW U LILL-KUMITAT TAR-REĠJUNI

Pjan ta’ Azzjoni Ewropew dwar iċ-ċibersigurtà tal-isptarijiet u tal-fornituri tal-kura tas-saħħa

1. Introduzzjoni

L-ambjent tas-sigurtà tal-UE qed jinbidel malajr, u qed jeskalaw l-attakki ibridi u l-attakki ċibernetiċi li jkunu maħsubin biex jiddestabbilizzaw is-soċjetà tagħna, biex jiżirgħu il-firda u t-tfixkil, iżda anki biex jagħmlu l-profitti miċ-ċiberkriminalità. Għalhekk, l-Ewropa trid issaħħaħ b'urġenza t-tħejjija u r-reżiljenza tagħha għal din ir-realtà l-ġdida, fis-setturi kollha u b'approċċ "tas-soċjetà kollha" u "ta' gvern sħiħ", kif mitlub fir-rapport tal-Konsulent Speċjali tal-President tal-Kummissjoni Ewropea, Sauli Niinistö.

Is-sistemi tal-kura tas-saħħa siguri u reżiljenti huma pedament tal-mudell soċjali tal-UE. Madankollu, l-isptarijiet u s-sistemi tal-kura tas-saħħa qed iġarrbu theddid dejjem akbar, b'mod partikolari minn klikek organizzati tar-ransomware li jattakkaw lil dawn imsemmija għall-gwadann finanzjarju, xprunati mill-valur kbir li għandha d-data tal-pazjenti, inkluż ir-rekords elettroniċi tas-saħħa. Is-settur tas-saħħa tabilħaqq sar l-aktar industrija attakkata fl-UE matul l-aħħar erba' snin, inkluż tul il-pandemija tal-COVID-19 meta l-infrastruttura tas-saħħa sfat dejjem aktar fil-mira tal-attakki ċibernetiċi. L-attakki ċibernetiċi fuq l-isptarijiet u l-fornituri tal-kura tas-saħħa qed jikkaġunaw ħsara diretta lin-nies, idewmu l-proċeduri mediċi, jikkawżaw konġestjonijiet fl-emerġenzi u jistgħu, f'każijiet estremi, iwasslu għat-telf tal-ħajjiet.

U r-riskji huma ferm akbar issa li s-settur qed issirlu trasformazzjoni diġitali vitali. Is-saħħa diġitali u l-użu u l-użu mill-ġdid tad-data dwar is-saħħa jistgħu jippermettu mudelli tal-kura aktar adattati għall-ħtiġijiet u l-preferenzi tan-nies u tal-pazjenti, għax jipprevjenu l-bidu tal-mard jew jippermettu trattament aktar bikri. L-integrazzjoni tal-għodod u s-soluzzjonijiet diġitali fil-proċessi kliniċi kif ukoll l-użu u l-użu mill-ġdid tad-data dwar is-saħħa jistgħu jinfurmaw aħjar lid-deċiżjonijiet kliniċi, jgħinu fl-awtomatizzazzjoni tas-saħħa, u anki għal kura tal-pazjenti aktar malajr u aħjar. L-għodod diġitali, l-użu tad-data, u l-apparati mediċi – li spiss ikunu konnessi mal-internet u mħaddma bl-intelliġenza artifiċjali (AI) – huma kruċjali wkoll biex jingħelbu ċerti sfidi bħall-iskarsezzi tal-professjonisti tal-kura tas-saħħa.

Fl-istess ħin, l-għodod diġitali jespandu wkoll il-miri potenzjali għaċ-ċiberkriminali. Barra minn hekk, ċerti atturi statali ma joqogħdux lura milli jpoġġu fil-mira tagħhom il-faċilitajiet tal-kura tas-saħħa, kif rajna fil-gwerra tal-aggressjoni Russa attwali kontra l-Ukrajna. Dan jagħmel lis-settur mira potenzjali għall-attakki ċibernetiċi bħala parti minn kampanja ibrida usa'. L-attakki ċibernetiċi mhux biss jipperikolaw is-sikurezza tal-pazjenti iżda anki jnaqqsu l-fiduċja pubblika fl-infrastruttura tas-saħħa u jikkaġunaw kostijiet sinifikanti tal-irkupru. Lil hinn mis-salvagwardja kontra l-attakki ċibernetiċi, l-infrastruttura diġitali reżiljenti u sigura hi essenzjali wkoll għall-appoġġ tal-implimentazzjoni u l-użu sħiħ tal-Ispazju Ewropew tad-Data dwar is-Saħħa[1] (EHDS).

Għalhekk, wasal iż-żmien li ngħollu l-livell u nsaħħu ċ-ċibersigurtà u r-reżiljenza tal-isptarijiet u tal-fornituri tal-kura tas-saħħa tal-Ewropa, kif enfasizzat mill-President von der Leyen fil-Linji Gwida Politiċi tagħha għall-Kummissjoni 2024-2029[2]. Dan il-pjan ta' azzjoni jwieġeb għall-urġenza tas-sitwazzjoni u għat-theddid uniku li qed jiffaċċja s-settur. M'hemm l-ebda soluzzjoni sempliċi għall-problema kkumplikata tal-isfidi taċ-ċibersigurtà fil-kura tas-saħħa. Minflok, il-pjan ta' azzjoni jappella għal prevenzjoni msaħħa, tħejjija, u approċċ aktar ikkoordinat għas-solidarjetà filwaqt li jiġi sfruttat l-għarfien espert tal-industrija Ewropea taċ-ċibersigurtà. Bħala tali, il-pjan ta' azzjoni jirrifletti l-approċċ tal-UE għas-sigurtà li se jkompli jiġi żviluppat u formalizzat fl-Istrateġija Ewropea għas-Sigurtà Interna li jmiss, filwaqt li jiddefinixxi rispons komprensiv kontra t-theddid kollu għas-sigurtà

1 https://www.consilium.europa.eu/mt/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/

2 https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

interna u jiffoka fuq il-kapaċità li jiġi antiċipat it-theddid, li jiġu evitati d-danni u li jiġu protetti n-nies, filwaqt li jaġixxi fil-livelli kollha b'approċċ "tas-soċjetà kollha".

Is-settur tas-saħħa jinkludi għadd wiesa' ta' entitajiet u atturi, fosthom sptarijiet, kliniċi, djar tal-kura, ċentri tar-riabilitazzjoni u diversi fornituri tal-kura tas-saħħa, flimkien mal-industrija farmaċewtika, medika u bijoteknoloġika, il-manifatturi tal-apparati mediċi, u l-istituzzjonijiet tar-riċerka dwar is-saħħa. Dan il-pjan ta' azzjoni jiffoka b'mod predominanti fuq iċ-ċibersigurtà tal-isptarijiet u tal-fornituri tal-kura tas-saħħa, mifhuma bħala persuna fiżika jew ġuridika – jew bħala entità oħra – li legalment tipprovdi l-kura tas-saħħa fit-territorju ta' Stat Membru[3]. L-isptarijiet u l-fornituri tal-kura tas-saħħa huma interdipendenti ma' entitajiet oħra tas-saħħa, u huma l-eqreb tan-nies. Fl-istess ħin, il-miżuri biex tissaħħaħ iċ-ċibersigurtà tal-isptarijiet u tal-fornituri tal-kura tas-saħħa jenħtieġ li jindirizzaw ukoll ir-riskji li jaffettwaw il-katina u l-ekosistema usa' tal-provvista, li jirriżultaw pereżempju minn entitajiet li jużaw data dwar is-saħħa għar-riċerka u t-tagħlim awtomatiku jew li jipproduċu apparati mediċi, b'mod partikolari apparati mediċi b'kapaċità diġitali li jaqbdu mal-internet jew ma' apparati oħra ("Internet tal-Oġġetti").

Filwaqt li s-sigurtà tas-sistemi tas-saħħa hi primarjament kompetenza nazzjonali, is-saħħa hi wkoll settur kritiku skont id-Direttiva dwar miżuri għal livell għoli komuni ta' ċibersigurtà madwar l-UE kollha (NIS 2)[4]. Iċ-ċiberkriminali u atturi oħra tat-theddid joperaw mingħajr fruntieri, u l-isfidi taċ-ċibersigurtà li jiffaċċjaw l-organizzazzjonijiet tal-kura tas-saħħa huma simili wkoll bejn Stat Membru u ieħor. Il-kooperazzjoni fil-livell Ewropew hi siewja għall-iskambju u ż-żieda tal-aqwa prattika fil-livell tal-UE u nazzjonali. Għalhekk, il-Pjan ta' Azzjoni jipproponi koordinazzjoni u miżuri fil-livell tal-UE, u jistieden ukoll lill-Istati Membri jieħdu azzjoni biex jagħmlu differenza fil-kura tas-saħħa u l-ekosistema tas-saħħa usa'.

L-enfasi tal-Pjan ta' Azzjoni hi fuq il-bini tal-kapaċitajiet tas-settur biex qabelxejn **ikunu evitati** l-inċidenti taċ-ċibersigurtà, għax il-prevenzjoni hi dejjem aħjar mill-kura. It-tieni, il-Pjan ta' Azzjoni jagħti dettalji dwar azzjonijiet li jtejbu l-iskambji tal-informazzjoni dwar iċ-ċibersigurtà u l-kapaċità li **jiġi identifikat** it-theddid ċibernetiku, ħalli jkun hemm rispons aktar malajr. It-tielet, jipprovdi miżuri għal **rispons** aħjar għall-inċidenti, u għall-**irkupru** minnhom. Fl-aħħar, il-Pjan ta' Azzjoni jipprevedi modi biex l-atturi tat-theddid ċibernetiku jiġu **skoraġġuti** milli jniedu attakki kontra s-sistemi tas-saħħa fl-Ewropa.

Il-Pjan ta' Azzjoni se jiġi implimentat id f'id mal-fornituri tal-kura tas-saħħa u mal-ekosistema usa' tas-saħħa, l-Istati Membri, u l-komunità taċ-ċibersigurtà. Dan l-approċċ kollaborattiv hu kruċjali biex jiġu definiti u rfinati aktar l-azzjonijiet li jħallu l-akbar impatt, ħalli l-fornituri tal-kura tas-saħħa kritiċi kollha tal-Ewropa jkunu jistgħu jibbenefikaw minnhom. Għalhekk ma' din il-Komunikazzjoni se titnieda konsultazzjoni komprensiva mal-partijiet ikkonċernati, l-industrija u l-Istati Membri. Il-kooperazzjoni internazzjonali hi importanti għaċ-ċibersigurtà minħabba n-natura mingħajr fruntieri u interkonnessa tat-theddid ċibernetiku. Anki l-pajjiżi tat-tkabbir u tal-viċinat u pajjiżi sħab strateġiċi oħra tal-UE jġarrbu theddid komparabbli għaċ-ċibersigurtà. Fl-aħħar mill-aħħar, anki dan jista' jipperikola s-sigurtà tal-infrastruttura kritika fl-UE. Għalhekk hu importanti li t-tagħlimiet miksuba tul l-implimentazzjoni tal-Pjan ta' Azzjoni jiġu riflessi wkoll fil-kooperazzjoni tal-UE mal-pajjiżi tat-tkabbir u ma' pajjiżi sħab oħra, fid-dawl tal-livelli tat-theddid li huma esposti għalihom rispettivament.

---

3 L-Artikolu 3, il-punt (g), tad-Direttiva 2011/24/UE tal-Parlament Ewropew u tal-Kunsill dwar l-applikazzjoni tad-drittijiet tal-pazjenti fil-qasam tal-kura tas-saħħa transkonfinali, https://eur-lex.europa.eu/legal-content/MT/TXT/?uri=celex%3A32011L0024

4 Id-Direttiva (UE) 2022/2555 tal-Parlament Ewropew u tal-Kunsill tal-14 ta' Diċembru 2022 dwar miżuri għal livell għoli komuni ta' ċibersigurtà madwar l-Unjoni kollha (id-Direttiva NIS 2), https://eur-lex.europa.eu/eli/dir/2022/2555

2. L-isfida taċ-ċibersigurtà tal-isptarijiet u l-fornituri tal-kura tas-saħħa

<u>*Theddid ċibernetiku għas-settur tas-saħħa*</u>

L-attakki ċibernetiċi qed jiżdiedu globalment u fl-UE, b'xenarju ta' theddid dejjem aktar kumpless u dinamiku. L-avvanzi fl-AI qed jipprovdu għodod saħħithom lill-atturi kriminali u malizzjużi biex iżidu l-preċiżjoni u l-impatt tal-operazzjonijiet tagħhom, iżda fl-istess ħin dawn l-avvanzi qed isawru mill-ġdid il-possibbiltajiet taċ-ċiberdifiża għax jippermettu azzjoni awtomatizzata u fil-ħin reali kontra l-attakki.

Ir-ransomware jibqa' sfida kritika taċ-ċibersigurtà fl-UE u globalment, b'rapport partikolari jistma kost annwali dinji ta' aktar minn EUR 250 biljun sal-2031[5]. Meta jattakkaw, il-kriminali tar-ransomware mhux biss jikkriptaw id-data tal-vittmi għar-riskatt iżda jiżvelaw dejjem aktar informazzjoni sensittiva biex jeżerċitaw pressjoni addizzjonali. Sfida prominenti oħra hi l-vulnerabbiltajiet fis-software u fil-hardware: skont l-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà (ENISA)[6], il-kura tas-saħħa hi s-settur li ddikjara l-aktar inċidenti tas-sigurtà relatati ma' vulnerabbiltajiet bħal dawn[7]. Fost theddid ieħor li qed jikber hemm l-attakki distribwiti li jwaqqfu s-servizz (DDoS), imfassla biex jgħabbu lil xi sistema fil-mira b'ħafna traffiku u jagħmluha inaċċessibbli għall-utenti leġittimi[8].

Is-settur tas-saħħa qed jiffaċċja xejriet simili ta' theddid taċ-ċibersigurtà, b'enfasi kbira fuq l-attakki ransomware. Skont l-ENISA, ir-ransomware kien jirrappreżenta 54% tal-inċidenti taċ-ċibersigurtà analizzati fis-settur tas-saħħa bejn l-2021 u l-2023. 83% tal-attakki kienu motivati finanzjarjament, xprunati mill-valur għoli tad-data dwar il-kura tas-saħħa, filwaqt li 10% tal-attakki kellhom motivazzjoni ideoloġika[9]. Bl-istess mod, rapport tal-Kummissjoni li sar fl-2024 sab li 71% tal-attakki li kellhom effett fuq il-kura tal-pazjenti, bħal dewmien fit-trattament, fid-dijanjożi u l-aċċess dgħajjef għas-servizzi tal-emerġenza, kienu tat-tip ransomware[10]. L-attakki ransomware jista' jkollhom effett ta' tfixkil partikolari fuq il-forniment tas-servizzi tal-kura tas-saħħa, u b'hekk ipoġġu s-sikurezza tal-pazjenti fir-riskju. Barra minn hekk, mal-attakki ransomware spiss ikun hemm teħid ta' data tal-pazjenti[11], li spiss tinkludi data sensittiva relatata mas-saħħa, u jinkisru d-drittijiet fundamentali tan-nies għall-protezzjoni tad-data personali.

Fl-istess ħin, biż-żieda fid-diġitalizzazzjoni tal-kura tas-saħħa, qed tikber ukoll il-firxa tal-attakki. Skont ir-Rapport dwar l-Istat tad-Deċennju Diġitali 2024, medja ta' 79% taċ-ċittadini tal-UE għandhom aċċess online għar-rekords elettroniċi tas-saħħa tagħhom fil-kura primarja[12]. Ir-rekords elettroniċi tas-saħħa, is-sistemi tal-informazzjoni klinika, is-sistemi tal-fluss tax-xogħol fl-isptarijiet, is-sistemi tal-IT għar-rimborż tat-trattamenti, is-sistemi tal-immaġnijiet mediċi, u l-apparati mediċi

---

5 Cybersecurity Ventures (l-1 ta' Ġunju 2024): "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031". https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

6 Ir-Regolament (UE) 2019/881tal-Parlament Ewropew u tal-Kunsill tas-17 ta' April 2019 dwar l-ENISA (l-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà) u dwar iċ-ċertifikazzjoni taċ-ċibersigurtà tat-teknoloġija tal-informazzjoni u tal-komunikazzjoni (l-Att dwar iċ-Ċibersigurtà), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

7 Ix-Xenarju tat-Theddid skont l-ENISA: is-Settur tas-Saħħa (Lulju 2023).

8 Ix-Xenarju tat-Theddid fl-2024 skont l-ENISA.

9 Ix-Xenarju tat-Theddid skont l-ENISA: is-Settur tas-Saħħa (Lulju 2023). Ir-rapport analizza l-fornituri tal-kura tas-saħħa, kif ukoll tipi oħra ta' organizzazzjonijiet, inkluż organizzazzjonijiet tar-riċerka fis-saħħa, manifatturi ta' ċerti prodotti relatati mas-saħħa, awtoritajiet tas-saħħa, organizzazzjonijiet tal-assigurazzjoni tas-saħħa, u faċilitajiet tat-trattament residenzjali u fornituri tas-servizzi soċjali. https://www.enisa.europa.eu/publications/health-threat-landscape

10 Il-Kummissjoni Ewropea: iċ-Ċentru Konġunt tar-Riċerka, Reina, V. u Griesinger, C., Cyber security in the health and medicine sector – A study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings, l-Uffiċċju tal-Pubblikazzjonijiet tal-UE, 2024, https://data.europa.eu/doi/10.2760/693487

11 Skont ix-Xenarju tat-Theddid skont l-ENISA: is-Settur tas-Saħħa, it-teħid jew is-serq tad-data ġew ikkonfermati fi 43% tal-inċidenti ransomware analizzati.

12 Ir-Rapport dwar l-Istat tad-Deċennju Diġitali 2024

użati għal skopijiet dijanjostiċi jew għall-monitoraġġ tal-pazjenti huma lkoll eżempji ta' għodod diġitali li jistgħu jaqdu rwol ewlieni biex tiżdied l-effiċjenza u titjieb il-prestazzjoni tas-settur tas-saħħa, iżda huma wkoll miri potenzjali tal-attakki taċ-ċibersigurtà. Ċerti attivitajiet speċifiċi tal-kura tas-saħħa bħall-kura intensiva u l-immaġnijiet radjoloġiċi, jew oqsma mediċi bħall-onkoloġija u l-kardjoloġija, li jiddependu ħafna fuq apparati attivati diġitalment, għandhom riskju partikolari ta' attakki ċibernetiċi. Barra minn hekk, ċerti kwistjonijiet tal-katina tal-provvista jistgħu jwasslu għax-xiri ta' apparati li ma jkollhomx sigurtà ċibernetika biżżejjed u dawn jaggravaw ir-riskji ġenerali eżistenti.

Pereżempju, tul il-pandemija tal-COVID-19, attakk ransomware partikolari pparalizza partijiet kbar tas-sistema tal-kura tas-saħħa Irlandiża, u wassal għall-kanċellazzjoni ta' xi servizzi f'31 mill-54 sptar akut[13]. Is-servizzi tas-saħħa kellhom jerġgħu lura għar-rekords stampati, u b'hekk naqset l-effiċjenza tal-operat. L-attakk oriġina minn email ta' phishing li nhemeż magħha kontenut malizzjuż[14]. L-inċident wera l-potenzjal li l-attakki ċibernetiċi jinfirxu f'sistemi differenti, u allura l-importanza li tiġi protetta l-firxa kollha li potenzjalment jolqot attakk fuq organizzazzjoni tal-kura tas-saħħa. L-attakk wera wkoll l-importanza li niżguraw il-kultura fundamentali taċ-ċiberiġjene u taċ-ċibersigurtà fl-organizzazzjonijiet kollha.

Il-maturità taċ-ċibersigurtà tal-isptarijiet u l-fornituri tal-kura tas-saħħa

Ix-xenarju tal-kura tas-saħħa fl-UE huvarjat ħafna, u l-isptarijiet u l-fornituri l-oħra tal-kura tas-saħħa madwar l-Istati Membri jvarjaw ħafna mil-lat ta' sjieda, struttura u daqs. Ġieli l-governanza tal-kura tas-saħħa tkun ibbażata fuq approċċ ċentralizzat fil-livell nazzjonali, u ġieli fil-livell reġjonali u lokali; ġieli l-fornituri tal-kura tas-saħħa jkollhom sidien pubbliċi u ġieli privati. Barra minn hekk, jeżistu wkoll differenzi fl-istess pajjiż, pereżempju meta jkollok disparitajiet soċjoekonomiċi u territorjali sinifikanti bejn ir-reġjuni li jwasslu għal xenarju kumpless. Dan ix-xenarju kumpless tal-kura tas-saħħa jaf jiġi sfidat bi kriżijiet tas-saħħa importanti, minħabba mard komunikabbli, bħall-pandemija tal-COVID-19, iżda hemm ukoll riskji oħra għas-saħħa pereżempju relatati mat-tibdil fil-klima. Fl-aħħar, hemm varjabbiltà u frammentazzjoni sinifikanti fil-livell tad-diġitalizzazzjoni u l-adozzjoni tat-teknoloġija min-naħa tal-fornituri tal-kura tas-saħħa. Eżempju ta' din il-kumplessità hu li l-waqfien tad-disponibbiltà tas-servizz ikkawżat bl-inċident ċibernetiku jista' jikkaġuna danni serji u jagħmel ħsara lill-pazjenti anke fil-faċilitajiet tal-kura tas-saħħa fuq skala żgħira, bħal kliniċi jew servizzi mediċi tal-emerġenza li jipprovdu servizz essenzjali lil għadd relattivament żgħir ta' persuni.

Skont ir-Rapport tal-ENISA tal-2024 dwar l-Istat taċ-Ċibersigurtà fl-Unjoni[15], il-maturità taċ-ċibersigurtà tas-settur tas-saħħa tal-UE hi moderata u hemm differenzi kbar fil-livell tal-maturità taċ-ċibersigurtà bejn l-entitajiet tal-kura tas-saħħa madwar l-Ewropa. Jistgħu jiġu osservati defiċjenzi f'oqsma ewlenin, fosthom nuqqas ta' riżorsi umani biżżejjed, l-għarfien tal-organizzazzjonijiet dwar il-ktajjen tal-provvista tat-teknoloġija tal-informazzjoni u tal-komunikazzjoni (ICT) tagħhom, u l-installazzjoni ta' elementi aġġornati tas-sigurtà fil-prodotti. Is-settur jitħabat ma' miżuri bażiċi taċ-ċiberiġjene u s-sigurtà fundamentali, kif juri l-fatt li kważi l-organizzazzjonijiet tas-saħħa kollha mistħarrġa jsibu sfidi biex jagħmlu valutazzjonijiet tar-riskju taċ-ċibersigurtà, filwaqt li kważi nofshom qatt ma wettqu analiżi tar-riskju[16].

---

13 L-Eżekuttiv tas-Servizz tas-Saħħa Irlandiż (2021): "Conti cyber attack on the HSE: Independent Post Incident Review."

14 L-Eżekuttiv tas-Servizz tas-Saħħa Irlandiż: "Cyber-attack and HSE response". https://www2.hse.ie/services/cyber-attack/what-happened/.

15 L-ENISA: ir-Rapport tal-2024 dwar l-Istat taċ-Ċibersigurtà tal-Unjoni (Settembru 2024). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

16 Ix-Xenarju tat-Theddid skont l-ENISA: is-Settur tas-Saħħa (Lulju 2023). https://www.enisa.europa.eu/publications/health-threat-landscape

Sfida sinifikanti oħra għaċ-ċibersigurtà tal-isptarijiet hi l-intersezzjoni tat-teknoloġija tal-informazzjoni (IT) u t-teknoloġija operazzjonali (OT), fejn hemm prijoritajiet tas-sigurtà differenti fir-rigward tal-kunfidenzjalità, id-disponibbiltà u l-affidabbiltà, u meta ksur f'qasam wieħed jista' jaffettwa lill-ieħor. Ir-Rapport tal-ENISA tal-2024 dwar l-Istat taċ-Ċibersigurtà fl-Unjoni jenfasizza wkoll li s-settur tas-saħħa mhux qed jaħdem kif xieraq biex jiżgura s-sigurtà tal-prodotti u l-proċessi tal-ICT li juża, għax hemm varjetà kbira ta' entitajiet, apparati u prodotti tas-saħħa.

Din id-diversità, flimkien mal-livelli differenti tat-tixrid tal-għarfien ċibernetiku fost il-persunal u l-maniġment tal-isptarijiet, toħloq sfida kumplessa biex tkun żgurata ċ-ċibersigurtà tas-sistemi tal-kura tas-saħħa. Pereżempju, skont l-Ewrobarometru tal-2024 dwar il-Ħiliet Ċibernetiċi, 25% biss tal-kumpaniji mistħarrġa fis-settur tas-saħħa, tal-edukazzjoni u tal-kura soċjali kienu taw taħriġ jew wasslu għarfien dwar iċ-ċibersigurtà fit-12-il xahar preċedenti[17]. Hemm bżonn azzjoni li trawwem kultura tat-tixrid tal-għarfien dwar iċ-ċibersigurtà fost il-professjonisti frontali fil-kura tas-saħħa. Pereżempju, ir-rotazzjonijiet tal-persunal, l-użu ta' stazzjonijiet tax-xogħol kondiviżi, il-ġestjoni ħażina tal-awtentikazzjoni, u l-użu ta' tagħmir tal-midja li jista' jitneħħa huma sorsi addizzjonali ta' vulnerabbiltajiet li jaffettwaw iċ-ċibersigurtà tal-fornituri tal-kura tas-saħħa[18].

F'ħafna każijiet, l-IT u l-OT jiġu esternalizzati mqar parzjalment. L-Ewrobarometru tal-2024 sab li s-sehem tal-kumpaniji li jesternalizzaw imqar xi aspetti taċ-ċibersigurtà tagħhom hu l-akbar fis-settur tas-saħħa, fl-edukazzjoni u fil-kura soċjali, b'57% tal-kumpaniji mistħarrġa jagħmlu dan[19]. Bl-istess mod, hemm xejra qawwija ta' migrazzjoni lejn il-cloud computing, xprunata mill-bżonn ta' ħżin u ġestjoni tad-data skalabbli, kosteffiċjenza, kollaborazzjoni aħjar, u appoġġ għat-teknoloġiji avvanzati bħall-AI u l-Internet tal-Oġġetti Mediċi. Fl-2022, 58% tal-organizzazzjonijiet tas-saħħa użaw pjattaforma tas-saħħa diġitali bbażata fuq il-cloud[20]. Iżda filwaqt li din il-bidla tista' ġġib effiċjenzi sinifikanti, tinvolvi wkoll riskji li jeħtieġu deċiżjonijiet infurmati waqt l-akkwist u konfigurazzjoni sigura.

Tisboq dawn l-isfidi kollha hemm il-kwistjoni tal-bini tal-kapaċità u l-finanzjament. Il-finanzjament għaċ-ċibersigurtà fis-settur tas-saħħa kien limitat u għadu sfida universali madwar l-UE[21]. Barra minn hekk, dawn l-isfidi tal-finanzjament jinħassu f'kuntest ta' popolazzjoni li qed tixjieħ u li fid-deċennji li ġejjin mistennija toħloq pressjonijiet baġitarji estensivi fuq is-sistemi tas-saħħa tal-Ewropa.

L-użu kontinwu ta' għodod obsoliti u s-sistemi ta' legat, ir-riżorsi limitati għall-prevenzjoni tal-inċidenti jew għar-rispons għalihom, u l-lakuni fil-maturità taċ-ċibersigurtà spiss jinħolqu minħabba nuqqasijiet ta' finanzjament. L-isptarijiet jiffaċċjaw sfida kontinwa biex isibu bilanċ bejn infrastruttura sigura u diġitali aġġornata u l-investimenti l-oħra meħtieġa biex itejbu l-kura tal-pazjenti, bħall-ingaġġ tat-tobba u professjonisti oħra tal-kura tas-saħħa, l-implimentazzjoni ta' metodi ġodda għad-dijanjożu u t-trattament, u l-akkwist ta' apparati ġodda. Skont l-ENISA[22], is-settur tas-saħħa jikklassifika biss fis-7 post minn 12-il settur studjati fejn jidħol il-proporzjon tal-infiq fuq is-sigurtà tal-informazzjoni mill-infiq totali fl-IT, b'medjan ta' 8,3% fis-settur tas-saħħa.

---

17 L-Ewrobarometru Flash 547 dwar il-Ħiliet Ċibernetiċi (Mejju 2024). https://europa.eu/eurobarometer/surveys/detail/3176

18 Panacea – People-centric cybersecurity in healthcare (2021): White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres.

19 L-Ewrobarometru Flash 547 dwar il-Ħiliet Ċibernetiċi (Mejju 2024). https://europa.eu/eurobarometer/surveys/detail/3176

20 L-ENISA: ir-Rapport tal-2022 dwar l-Investimenti tan-NIS (Novembru 2022). https://www.enisa.europa.eu/publications/nis-investments-2022

21 L-organizzazzjoni u l-għoti tas-servizzi tas-saħħa u tal-kura medika huma kompetenza nazzjonali skont l-Artikolu 168 tat-Trattat dwar il-Funzjonament tal-Unjoni Ewropea, u l-finanzjament tas-sistemi tal-kura tas-saħħa jvarja fost l-Istati Membri.

22 L-ENISA: ir-Rapport tal-2022 dwar l-Investimenti tan-NIS (Novembru 2022). https://www.enisa.europa.eu/publications/nis-investments-2022.

3. Iċ-Ċentru Ewropew ta' Appoġġ għaċ-Ċibersigurtà għall-isptarijiet u l-fornituri tal-kura tas-saħħa

Il-qafas taċ-ċibersigurtà tal-UE joffri firxa wiesgħa ta' għodod li jenħtieġ li jiġu sfruttati biex jittejbu s-sigurtà u r-reżiljenza tal-isptarijiet u tal-fornituri tal-kura tas-saħħa. Biex jiġu indirizzati d-diversi sfidi enfasizzati hawn fuq, jeħtieġ jiġi żviluppat approċċ strateġiku unifikat fil-livell tal-UE li jiġbor flimkien ir-riżorsi, l-għarfien espert u l-għodod meħtieġa biex it-theddid ċibernetiku jiġi indirizzat b'mod effettiv. Ħarsa ġenerali komprensiva, kif ukoll ippjanar u koordinazzjoni aħjar, huma essenzjali biex jgħinu lill-fornituri tal-kura tas-saħħa madwar l-UE jsaħħu d-difiżi tagħhom. Għal dan il-għan, l-ENISA tinsab fl-aħjar pożizzjoni biex fi ħdan l-organizzazzjoni tagħha tistabbilixxi **Ċentru Ewropew ta' Appoġġ għaċ-Ċibersigurtà għall-isptarijiet u l-fornituri tal-kura tas-saħħa**[23] bħala parti mill-mandat tagħha[24] biex tissalvagwardja u tappoġġa l-infrastruttura kritika tal-UE.

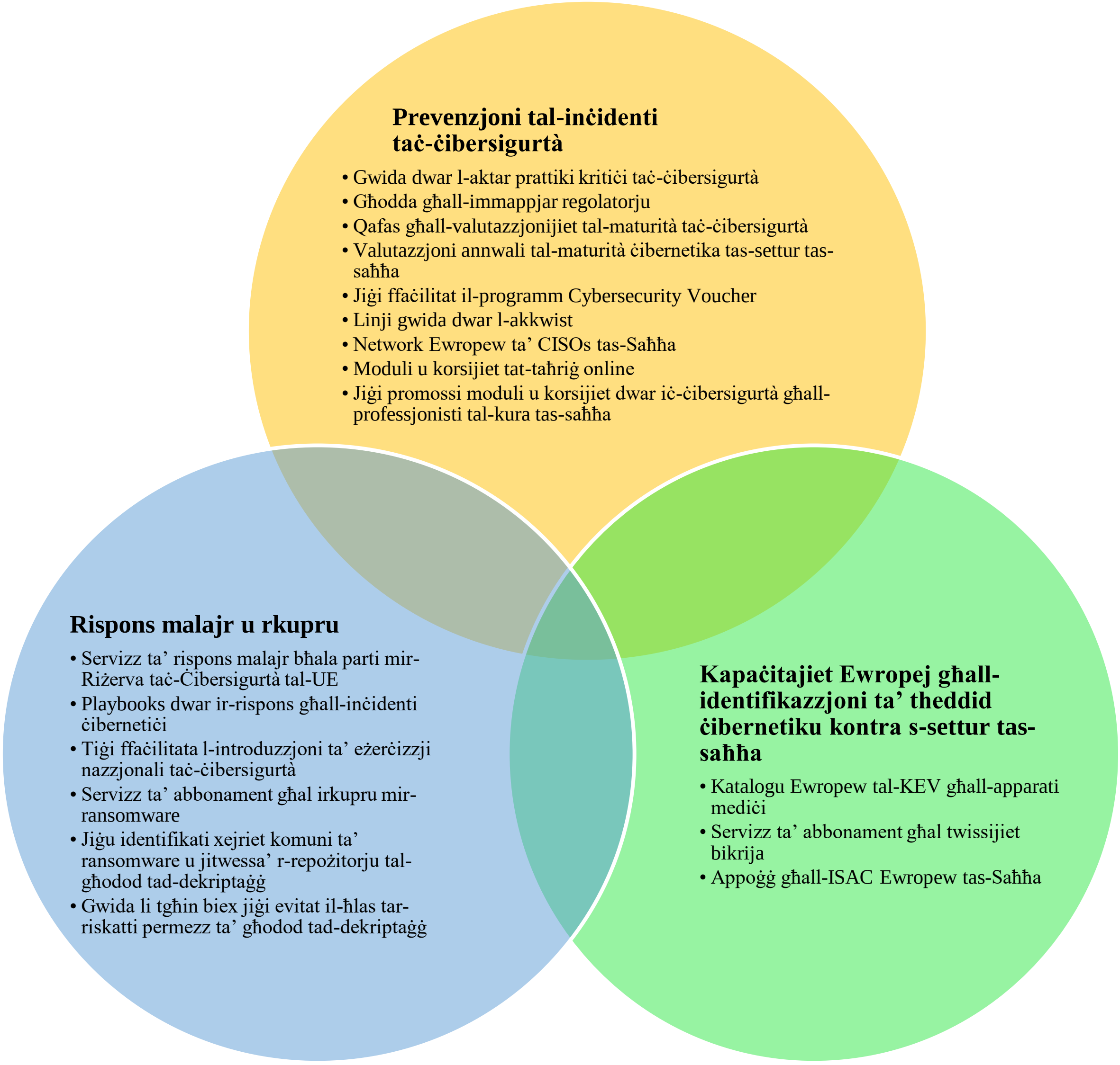
Iċ-Ċentru ta' Appoġġ għandu **jiżviluppa katalogu progressivament tas-servizzi komprensivi li jissodisfaw il-ħtiġijiet tal-isptarijiet u tal-fornituri tal-kura tas-saħħa**, u jiddeskrivi l-firxa tas-servizzi disponibbli għat-tħejjija, il-prevenzjoni, id-detezzjoni u r-rispons. B'ħidma mal-awtoritajiet tal-Istati Membri u abbażi tal-esperjenzi tal-isptarijiet u l-fornituri tal-kura tas-saħħa, iċ-Ċentru ta' Appoġġ għandu jiżviluppa repożitorju, b'aċċess u użu faċli għall-utenti, li jkun fih l-istrumenti kollha disponibbli fil-livelli Ewropej, nazzjonali u reġjonali. Fit-twettiq tal-attivitajiet tiegħu, dan jenħtieġ li jiżgura koordinazzjoni xierqa mal-Istati Membri, u jappoġġa l-prijoritizzazzjoni u t-twettiq ta' azzjonijiet kif meħtieġ fil-ħin reali.

Bħala sies importanti għall-iżvilupp tal-katalogu tas-servizzi taċ-Ċentru ta' Appoġġ, il-Kummissjoni se tipproponi li tniedi proġetti pilota madwar l-UE biex tiżviluppa l-aqwa prattiki għaċ-ċiberiġjene u l-valutazzjoni tar-riskji għas-sigurtà, u biex tindirizza l-ħtieġa għal monitoraġġ kontinwu taċ-ċibersigurtà, l-intelligence dwar it-theddid u r-rispons għall-inċidenti permezz ta' soluzzjonijiet taċ-ċibersigurtà mill-aktar avvanzati. L-eżiti ta' dawn il-proġetti pilota ffinanzjati mill-programm Ewropa Diġitali u mwettqa miċ-Ċentru Ewropew ta' Kompetenza Industrijali, Teknoloġika u tar-Riċerka fil-qasam taċ-Ċibersigurtà (ECCC) se jservu ta' tagħrif għal aktar azzjonijiet fil-livell tal-UE, inkluż għall-ħidma taċ-Ċentru ta' Appoġġ.

---

[23] F'dan id-dokument, "Ċentru ta' Appoġġ" tintuża b'mod interkambjabbli.

[24] Ir-Regolament (UE) 2019/881 tal-Parlament Ewropew u tal-Kunsill tas-17 ta' April 2019 dwar l-ENISA (l-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà) u dwar iċ-ċertifikazzjoni taċ-ċibersigurtà tat-teknoloġija tal-informazzjoni u tal-komunikazzjoni u li jħassar ir-Regolament (UE) Nru 526/2013 (l-Att dwar iċ-Ċibersigurtà), ĠU L 151, 7.6.2019, p. 15-69.



Illustrazzjoni 1: Kunċetti għall-katalogu tas-servizzi taċ-Ċentru ta' Appoġġ għall-isptarijiet u l-fornituri tal-kura tas-saħħa

3.1. Prevenzjoni tal-inċidenti taċ-ċibersigurtà

Azzjonijiet sempliċi li jbiddlu x-xenarju

Ċerti miżuri bażiċi taċ-ċibersigurtà, fosthom li niżguraw li s-sistemi jinżammu aġġornati, il-ġestjoni tal-backups, u li jkollna awtentikazzjoni b'diversi fatturi jistgħu, skont stima waħda, jipproteġu lill-organizzazzjonijiet minn sa 98% tal-attakki[25]. Ħafna mill-aktar miżuri taċ-ċiberiġjene u tal-ġestjoni tar-riskji li jħallu impatt huma relattivament sempliċi biex jiġu adottati, u b'hekk iċ-ċibersigurtà tista' titjieb faċilment. Għalhekk, wieħed mir-rwoli ewlenin taċ-Ċentru ta' Appoġġ jenħtieġ li jkun li **jiżviluppa gwida ċara u mmirata li tenfasizza l-aktar prattiki kritiċi taċ-ċibersigurtà u tgħin lill-fornituri tal-kura tas-saħħa fl-implimentazzjoni tagħhom**. Dan l-appoġġ irid jestendi lil hinn mill-isptarijiet il-kbar u jkun fih pariri wkoll imfasslin għall-entitajiet iżgħar, bħal għall-uffiċċji lokali tat-tobba tal-familja u l-kliniċi speċjalizzati, li ħafna drabi ma jkollhomx ir-riżorsi għal timijiet taċ-

[25] Il-Microsoft Digital Defense Report 2022. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

ċibersigurtà ddedikati iżda huma daqstant ieħor vulnerabbli għall-attakki. Barra minn hekk, jeħtieġ titqies l-importanza reġjonali ta' entitajiet speċifiċi tal-kura tas-saħħa biex tkun żgurata l-kura tal-pazjenti, pereżempju f'żoni mhux popolati. Anki l-istituti tar-riċerka dwar is-saħħa li jittrattaw ammonti kbar ta' data personali sensittiva jistgħu jibbenefikaw jekk jirċievu gwida dwar miżuri bażiċi taċ-ċibersigurtà li jtejbu r-reżiljenza tagħhom.

L-organizzazzjonijiet tal-kura tas-saħħa huma soġġetti wkoll għal firxa ta' obbligi relatati maċ-ċibersigurtà li joħorġu mil-leġiżlazzjoni tal-UE[26]. Filwaqt li l-obbligi huma kruċjali biex niżguraw linja bażi komuni għolja għaċ-ċibersigurtà u s-sigurtà tad-data, hu essenzjali li niżguraw li x-xenarju regolatorju ma jkunx diffiċli u peżanti bla bżonn biex wieħed josservah. Enfasi qawwija fuq il-konformità m'għandiex tmur kontra l-objettiv li titrawwem kultura soda taċ-ċibersigurtà. **Għodda tal-immappjar regolatorju b'aċċess faċli tista' tgħin biex jitnaqqas il-piż amministrattiv minn fuq l-entitajiet li huma soġġetti għal diversi strumenti regolatorji**. Apparti jiżviluppa gwida u settijiet tal-għodod, iċ-Ċentru ta' Appoġġ għandu jaħdem mill-qrib mal-Kummissjoni u mal-Istati Membri biex jiżviluppa u jxerred dik l-għodda malajr kemm jista' jkun. Għalhekk, iċ-Ċentru ta' Appoġġ se jkollu r-rwol importanti li r-regoli taċ-ċibersigurtà jagħmilhom sempliċi biex jinftiehmu u biex jiġu implimentati, pereżempju billi jipprovdi gwida għall-implimentazzjoni[27] u meta meħtieġ jippromwovi standards rilevanti.

Il-**Kartieri Ewropej tal-Identità Diġitali** li ġejjin huma għodda oħra biex tiġi ffaċilitata l-implimentazzjoni sempliċi ta' prattiki tajbin taċ-ċiberiġjene. Hu essenzjali li tonqos id-dipendenza fuq mekkaniżmi tal-identifikazzjoni dgħajfin, bħall-passwords, biex jonqsu r-riskji ta' aċċess mhux awtorizzat għad-data dwar is-saħħa. Minflok, hu kritiku li mmorru għal soluzzjonijiet siguri tal-awtentikazzjoni bbażati fuq identifikazzjoni affidabbli. Il-Kartiera Ewropea tal-Identità Diġitali toffri approċċ armonizzat għall-UE kollha għall-identifikazzjoni elettronika tal-professjonisti tal-kura tas-saħħa, u din se tipprovdi soluzzjoni soda u unifikata minn tmiem l-2026. Is-sistemi online kollha tal-informazzjoni dwar is-saħħa li jeħtieġ ikollhom awtentikazzjoni soda tal-utenti se jkunu obbligati jaċċettaw il-Kartiera għal skopijiet ta' identifikazzjoni minn tmiem l-2027[28].

---

26 Bħad-Direttiva NIS 2; ir-Regolament (UE) 2024/2847 tal-Parlament Ewropew u tal-Kunsill tat-23 ta' Ottubru 2024 dwar ir-rekwiżiti orizzontali taċ-ċibersigurtà għall-prodotti b'elementi diġitali (Att dwar ir-Reżiljenza Ċibernetika), http://data.europa.eu/eli/reg/2024/2847/ojhttp://data.europa.eu/eli/reg/2024/2847/oj; ir-Regolament (UE) 2017/745 tal-Parlament Ewropew u tal-Kunsill tal-5 ta' April 2017 dwar apparati mediċi, http://data.europa.eu/eli/reg/2017/745/ojhttp://data.europa.eu/eli/reg/2017/745/oj (ir-Regolament dwar l-Apparati Mediċi), http://data.europa.eu/eli/reg/2017/745/oj, ir-Regolament dwar l-Apparati Mediċi; ir-Regolament (UE) 2017/746 tal-Parlament Ewropew u tal-Kunsill tal-5 ta' April 2017 dwar apparati mediċi dijanjostiċi *in vitro* (ir-Regolament dwar l-apparati mediċi dijanjostiċi *in vitro*), http://data.europa.eu/eli/reg/2017/746/ojhttp://data.europa.eu/eli/reg/2017/746/oj; ir-Regolament (UE) 2016/679 tal-Parlament Ewropew u tal-Kunsill tas-27 ta' April 2016 dwar il-protezzjoni tal-persuni fiżiċi fir-rigward tal-ipproċessar ta' data personali u dwar il-moviment liberu ta' tali data (ir-Regolament Ġenerali dwar il-Protezzjoni tad-Data), https://eur-lex.europa.eu/legal-content/MT/TXT/?uri=CELEX%3A32016R0679&qid=1737008246921https://eur-lex.europa.eu/legal-content/MT/TXT/?uri=CELEX%3A32016R0679&qid=1737008246921; ir-Regolament (UE) 2024/1689 tal-Parlament Ewropew u tal-Kunsill tat-13 ta' Ġunju 2024 li jistabbilixxi regoli armonizzati dwar l-intelliġenza artifiċjali (l-Att dwar l-Intelliġenza Artifiċjali), https://eur-lex.europa.eu/legal-content/MT/TXT/?uri=CELEX%3A32024R1689&qid=1737008376857; il-Proposta għal REGOLAMENT TAL-PARLAMENT EWROPEW U TAL-KUNSILL dwar l-Ispazju Ewropew tad-Data dwar is-Saħħa, COM(2022)197 final, https://eur-lex.europa.eu/legal-content/MT/TXT/?uri=celex%3A52022PC0197. In-negozjati ngħalqu bi ftehim politiku fir-rebbiegħa tal-2024 u, wara l-finalizzazzjoni, il-pubblikazzjoni fil-Ġurnal Uffiċjali hija mistennija għar-rebbiegħa tal-2025

27 L-iżvilupp ta' linji gwida dwar l-interpretazzjoni tar-Regolament Ġenerali dwar il-Protezzjoni tad-Data (GDPR) jaqa' fir-responsabbiltà tal-Bord Ewropew għall-Protezzjoni tad-Data (EDPB). L-iżvilupp ta' gwida mill-ENISA għandu jirrispetta bis-sħiħ il-prerogattivi tal-EDPB.

28 L-Artikolu 5(f)(1)-(2) tar-Regolament (UE) Nru 910/2014.

Tħejjija u Appoġġ Immirat

L-ittestjar tat-tħejjija, li jinvolvi azzjonijiet bħall-ittestjar tal-penetrazzjoni, hu pedament għal ċibersigurtà effettiva, u l-Kummissjoni diġà allokat finanzjament lill-ENISA għal inizjattivi pilota tat-tħejjija, li ħarġu fid-dieher kif is-settur tas-saħħa hu fost l-aktar oqsma li jeħtieġu ttestjar u valutazzjonijiet ulterjuri biex jiġu identifikati l-lakuni fil-maturità taċ-ċibersigurtà. Bid-dħul fis-seħħ tal-Att dwar iċ-Ċibersolidarjetà, dawn l-isforzi se jespandu ġmielhom u t-tmexxija se tkun f'idejn l-ECCC. Biex tindirizza din il-ħtieġa, wara konsultazzjoni mal-Grupp ta' Kooperazzjoni tan-NIS, mal-EU-CyCLONe[29] u mal-ENISA, il-Kummissjoni se tipproponi li s-settur tas-saħħa jiġi identifikat bħala settur li jista' jikseb appoġġ għall-**ittestjar ikkoordinat tat-tħejjija** skont l-Att dwar iċ-Ċibersolidarjetà. Barra minn hekk, iċ-Ċentru ta' Appoġġ jenħtieġ li jiżviluppa **qafas imfassal apposta għall-valutazzjonijiet tal-maturità taċ-ċibersigurtà speċifiċi għall-kura tas-saħħa**. Dawn il-valutazzjonijiet tal-maturità jipprovdu għarfien azzjonabbli lill-entitajiet dwar il-vulnerabbiltajiet tagħhom u jippermettulhom juru t-tħejjija tagħhom għaċ-ċibersigurtà lill-pazjenti u lill-partijiet ikkonċernati, filwaqt li jibnu l-fiduċja fis-servizzi tagħhom. F'livell aggregat, iċ-Ċentru ta' Appoġġ għandu jwettaq **Valutazzjoni tal-Maturità Ċibernetika tas-Saħħa kull sena**, li tagħti ħarsa ġenerali ċara taċ-ċibersigurtà tas-settur tas-saħħa kemm fil-livell nazzjonali kif ukoll tal-UE.

Is-settur tas-saħħa jiddependi ħafna fuq il-kuntratturi esterni fejn jidħlu s-servizzi taċ-ċibersigurtà[30], u dan jixhed il-bżonn ta' appoġġ immirat biex jissaħħu d-difiżi. Filwaqt li jibnu fuq inizjattivi li rnexxew bħall-Vawċers tal-Innovazzjoni tal-UE, **l-Istati Membri għandhom jikkunsidraw miżuri mmirati bħall-Vawċers taċ-Ċibersigurtà għall-isptarijiet u l-fornituri tal-kura tas-saħħa mikro, żgħar u medji**. Dawn il-vawċers jipprovdu assistenza finanzjarja biex jiddaħħlu miżuri speċifiċi taċ-ċibersigurtà. Il-prijoritizzazzjoni tal-allokazzjoni tal-vawċers għandha tiġi infurmata mis-sejbiet tal-ittestjar tat-tħejjija u l-valutazzjonijiet tal-maturità.

L-għarfien u l-kuntest lokali huma kruċjali għall-introduzzjoni effettiva tal-vawċers jew ta' programmi oħra ta' appoġġ, biex b'hekk ikunu żgurati r-rilevanza u l-aċċessibbiltà. Il-fondi tal-UE, bħall-Fond Ewropew għall-Iżvilupp Reġjonali, diġà huma attivi fl-appoġġ tal-inizjattivi taċ-ċibersigurtà u tas-saħħa diġitali, u għalhekk jistgħu jkunu mezz għall-iżvilupp ta' skemi ta' vawċers taċ-ċibersigurtà mmirati għall-fornituri tal-kura tas-saħħa. Biex jixpruna dan l-isforz, iċ-Ċentru ta' Appoġġ għandu jikkollabora mal-Istati Membri u l-awtoritajiet reġjonali tal-programm biex jappoġġa l-iżvilupp ta' dawn l-iskemi tal-vawċers reġjonali, u biex jibni fuq it-tagħlimiet tal-proġetti nazzjonali eżistenti u fuq l-azzjonijiet iffinanzjati mill-programm Ewropa Diġitali ħalli jiżgura implimentazzjoni prattika u li tħalli l-impatt.

Barra minn hekk, mill-2014 'il quddiem, il-programmi ta' Orizzont kienu strumentali għall-finanzjament ta' firxa ta' inizjattivi tar-riċerka ffukati fuq it-tisħiħ tar-reżiljenza tal-istituzzjonijiet tal-kura tas-saħħa, bħall-isptarijiet, kontra t-theddid ċibernetiku u l-mitigazzjoni tar-riskji assoċjati mal-użu ħażin tat-teknoloġiji emerġenti. Fost ir-riżultati tanġibbli miksuba hemm sett ta' għodod, oqfsa u sistemi speċjalizzati, bħal għodod tal-valutazzjoni tar-riskju, pjattaformi għall-kondiviżjoni tad-data li jħarsu l-privatezza, soluzzjonijiet kriptografiċi, programmi tat-taħriġ u t-tixrid tal-għarfien dwar iċ-ċibersigurtà, u sistemi tad-detezzjoni tat-theddid fil-ħin reali. B'mod partikolari, dawn is-soluzzjonijiet ġew ivvalidati b'mod rigoruż b'implimentazzjonijiet pilota fid-dinja reali f'ambjenti tal-kura tas-saħħa, u żguraw l-effettività u l-applikabbiltà prattika tagħhom fil-protezzjoni mit-theddid ċibernetiku.

[29] In-Network Ewropew tal-organizzazzjonijiet ta' kollegament f'każ ta' ċiberkriżi

[30] Ara r-Rapport tal-ENISA dwar l-Investimenti tan-NIS 2023 (Novembru 2023) li jenfasizza l-prominenza tal-appoġġ estern għall-awditjar u l-konformità taċ-ċibersigurtà. https://www.enisa.europa.eu/publications/nis-investments-2023

Sigurtà għall-Ktajjen tal-Provvista tal-Kura tas-Saħħa

Sfida ewlenija għall-organizzazzjonijiet tal-kura tas-saħħa hi l-ġestjoni tal-ktajjen tal-provvista kumplessi tal-ICT, li jinvolvu firxa ta' prodotti bħal apparati mediċi konnessi, sistemi ta' Rekords Elettroniċi tas-Saħħa u hardware tal-uffiċċju. L-isptarijiet u l-fornituri tal-kura tas-saħħa jeħtieġu sistemi u servizzi tal-ICT affidabbli u siguri għall-operat tagħhom. Biex jgħinhom jindirizzaw l-isfidi taċ-ċibersigurtà fis-settur tas-saħħa, il-Grupp ta' Kooperazzjoni tan-NIS għandu jwettaq **valutazzjoni kkoordinata tar-riskji għas-sigurtà, filwaqt li jivvaluta r-riskji tekniċi u strateġiċi relatati mal-ktajjen tal-provvista tal-apparati mediċi u jipproponi miżuri tal-mitigazzjoni.**[31] Kif xieraq, il-Grupp ta' Kooperazzjoni tan-NIS għandu jikkollabora mal-Grupp ta' Koordinazzjoni tal-Apparat Mediku.

L-Att dwar ir-Reżiljenza Ċibernetika hu qafas ġdid u komprensiv li jistabbilixxi r-rekwiżiti taċ-ċibersigurtà għall-ippjanar, id-disinn, l-iżvilupp, kif ukoll it-trattament, it-traqqigħ, u r-rapportar tal-vulnerabbiltajiet sfruttati b'mod attiv fir-rigward ta' kważi l-prodotti kollha tal-hardware u tas-software, f'kull stadju tal-katina tal-valur[32]. L-apparati mediċi huma tip ta' prodott użat f'wieħed mill-aktar oqsma sensittivi tas-soċjetà tagħna. Ir-rekwiżiti taċ-ċibersigurtà għal dawn il-prodotti joħorġu mir-Regolament dwar l-Apparati Mediċi preeżistenti u r-Regolament dwar l-Apparati Mediċi Dijanjostiċi *in vitro*[33]. L-evalwazzjoni li għaddejja ta' dawk ir-regolamenti qed teżamina l-potenzjal ta' koerenza u sinerġiji akbar bejn dawn l-oqfsa biex jiġu ggarantiti s-simplifikazzjoni u ċibersigurtà mill-aktar avvanzata.

Barra minn hekk, is-sejbiet tal-valutazzjoni tar-riskji għandhom jappoġġaw lill-organizzazzjonijiet tal-kura tas-saħħa fir-rieżami tal-prattiki taċ-ċibersigurtà tal-katina tal-provvista tagħhom kif meħtieġ skont id-Direttiva NIS 2, u jistgħu jinfurmaw l-iżvilupp ta' **Linji Gwida ġodda dwar l-Akkwist**[34]. Żviluppati mill-ENISA permezz taċ-Ċentru ta' Appoġġ tagħha, dawn il-linji gwida għandhom jirriflettu x-xejriet riċenti, bħall-cloudification tal-ħżin tad-data tal-pazjenti, inkluż il-ħtieġa għal migrazzjoni sigura tad-data tas-saħħa elettronika lejn ambjenti tal-cloud. Barra minn hekk, il-Linji Gwida l-ġodda għandhom joffru għodod prattiċi lill-organizzazzjonijiet biex iżommu rekord tal-ktajjen tal-provvista tagħhom, inkluż il-fornituri tas-servizzi tas-sigurtà ġestiti (MSSPs), ir-rapporti tal-attestazzjoni jew il-valutazzjonijiet tar-riskju ta' partijiet terzi.

Għall-cloud, hemm bżonn aktar azzjoni biex jingħelbu l-isfidi uniċi tal-ġestjoni tad-data sensittiva dwar il-kura tas-saħħa, inkluż sigurtà akbar, privatezza, u riskji operazzjonali. Biex jissaħħu s-salvagwardji, l-esperti jirrakkomandaw l-inkorporazzjoni tas-"Sigurtà Prestabbilita u mid-Disinn" fis-servizzi tal-cloud. Dan l-approċċ jipprijoritizza l-infrastruttura sigura, il-ġestjoni proattiva tal-vulnerabbiltà, u taħlita ta' soluzzjonijiet governattivi u privati tal-cloud. Il-monitoraġġ kontinwu u l-attestazzjonijiet speċifiċi għall-bejjiegħ – bħaċ-ċertifikazzjonijiet tal-fornitur tas-sigurtà u l-awditjar tal-konformità mal-istandards nazzjonali u internazzjonali – huma essenzjali wkoll biex ikunu żgurati prattiki tas-sigurtà sodi.

---

31 Skont l-Artikolu 22 tad-Direttiva NIS 2.

32 Bħala l-ewwel pass, mill-1 ta' Awwissu 2025, ċerti kategoriji wiesgħa ta' tagħmir tar-radju, li mhumiex fil-kamp ta' applikazzjoni tar-Regolament dwar l-Apparati Mediċi u tar-Regolament dwar l-apparati mediċi dijanjostiċi *in vitro*, se jkunu meħtieġa jikkonformaw mar-rekwiżiti essenzjali tad-Direttiva dwar it-Tagħmir tar-Radju li huma relatati maċ-ċibersigurtà meta jiġu introdotti fis-Suq Uniku. Imbagħad, fil-11 ta' Diċembru 2027 se jidħol fis-seħħ l-Att dwar ir-Reżiljenza Ċibernetika.

33 F'Diċembru 2019, il-Grupp ta' Kooperazzjoni dwar l-Apparati Mediċi ħareġ gwida dwar iċ-ċibersigurtà għall-apparati mediċi, li tappoġġa lill-manifatturi biex jissodisfaw ir-rekwiżiti tal-Anness I taż-żewġ Regolamenti: https://ec.europa.eu/docsroom/documents/41863.

34 Building on the 2020 ENISA Procurement Guidelines for Cybersecurity in Hospitals (Frar 2020). https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

Għal servizzi bħall-Infrastruttura bħala Servizz (IaaS), il-Pjattaforma bħala Servizz (PaaS), u s-Software bħala Servizz (SaaS), l-implimentazzjoni tas-sigurtà spiss taqa' f'ħoġor il-klijent. Iżda ħafna organizzazzjonijiet tal-kura tas-saħħa m'għandhomx ir-riżorsi biex jissodisfaw dawn ir-rekwiżiti waħedhom. Biex dan jiġi indirizzat, **il-fornituri tas-servizzi tal-cloud għandhom jitħeġġu jimplimentaw ċerti miżuri tas-sigurtà bażi bħala karatteristika standard**. Dawn il-miżuri jnaqqsu r-riskju ta' konfigurazzjonijiet ħżiena, iżommu protezzjoni konsistenti fl-ambjenti ġestiti mill-klijenti, u jipprovdu assigurazzjoni akbar lill-utenti. L-istabbiliment ta' sigurtà bażi prestabbilita jkollu l-għan li jsib bilanċ bejn il-protezzjoni soda u l-prattiċità ħalli jiżgura l-użabbiltà lil firxa wiesgħa ta' organizzazzjonijiet tal-kura tas-saħħa. Dan l-isforz jinvolvi kollaborazzjoni mill-qrib bejn il-fornituri tal-cloud u s-settur tas-saħħa, filwaqt li jitħaddmu l-aqwa prattiki tal-industrija biex jinħolqu soluzzjonijiet effettivi u skalabbli.

Taħriġ u żvilupp tal-ħiliet

Biex l-Ewropa jkollha tkabbir u kompetittività sostenibbli fit-tul u servizzi ta' kwalità kbira, inkluż servizzi tal-kura tas-saħħa, hu importanti li jkollha forza tax-xogħol bil-ħiliet mitluba. L-iskarsezzi tal-professjonisti kwalifikati fiċ-ċibersigurtà huma sfida sinifikanti għall-Ewropa, b'nuqqas stmat ta' 299,000 professjonist biex jimlew il-ħtiġijiet tal-forza tax-xogħol fl-UE[35]. Skont l-Ewrobarometru tal-2024 dwar il-Ħiliet Ċibernetiċi[36], 81% tal-kumpaniji jqisu d-diffikultajiet biex jimpjegaw persunal taċ-ċibersigurtà bħala riskju ewlieni għal attakki ċibernetiċi potenzjali. Fis-setturi tal-edukazzjoni, tas-saħħa u tax-xogħol soċjali, 66% tar-rwoli taċ-ċibersigurtà jimtlew minn impjegati li jkunu ġejjin minn pożizzjonijiet mhux taċ-ċibersigurtà, u dan jenfasizza l-ħtieġa urġenti ta' taħriġ mill-ġdid u titjib tal-ħiliet.

Biex jindirizza din l-isfida, iċ-Ċentru ta' Appoġġ għandu jikkollabora mal-Konsorzju għall-Infrastruttura Diġitali Ewropea (EDIC) futur tal-ħiliet taċ-ċibersigurtà previst fil-Komunikazzjoni tal-Kummissjoni dwar l-Akkademja tal-Ħiliet fiċ-Ċibersigurtà[37]. Il-ħidma għandha tiffaċilita l-iskambji bejn il-professjonisti taċ-ċibersigurtà fis-settur tas-saħħa, bħall-Uffiċjali Kapijiet tas-Sigurtà tal-Informazzjoni (CISOs). Azzjoni potenzjali partikolari tkun li jinħoloq **Network Ewropew ta' CISOs tas-Saħħa**, li jibda bi grupp ta' esperti biex jaqsmu u jiżviluppaw l-aqwa prattiki, strateġiji għaż-żamma tat-talenti, u soluzzjonijiet biex aktar professjonisti taċ-ċibersigurtà jersqu lejn is-settur tas-saħħa. Barra minn hekk, taħt il-kappa tal-Akkademja tal-Ħiliet fiċ-Ċibersigurtà, għandhom jiġu żviluppati riżorsi biex tissaħħaħ il-forza tax-xogħol taċ-ċibersigurtà fis-settur tas-saħħa bl-appoġġ tal-industrija u tal-akkademja. F'dan ir-rigward, il-partijiet ikkonċernati tal-industrija għandhom jitħeġġu jiegħdu l-appoġġ tagħhom biex jissaħħaħ it-taħriġ fiċ-ċibersigurtà.

L-iżball uman għadu kontributur ewlieni għall-inċidenti taċ-ċibersigurtà fil-kura tas-saħħa, u dan jisħaq il-ħtieġa kritika ta' taħriġ komprensiv tal-persunal u tixrid tal-għarfien ċibernetiku. Peress li l-professjonisti tal-kura tas-saħħa jużaw sikwit l-għodod diġitali, hu vitali li dawn jiksbu għarfien dwar prattiki siguri. It-taħriġ immirat u l-kampanji tat-tixrid tal-għarfien jistgħu jnaqqsu r-riskji b'mod sinifikanti. Biex jindirizza dan, iċ-Ċentru ta' Appoġġ għandu jaħdem mal-professjonisti u l-fornituri tal-kura tas-saħħa, u jikkoopera mal-fornituri tal-edukazzjoni u t-taħriġ, l-industrija, l-EDIC tal-ħiliet taċ-ċibersigurtà u mal-awtoritajiet tal-Istati Membri biex joħloq u jxerred **moduli u korsijiet tat-taħriġ online li jkunu estensivi u faċli biex jiġu aċċessati**.

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Digital Skills and Jobs Platform

[36] L-Ewrobarometru Flash 547 dwar il-Ħiliet Ċibernetiċi.

[37] Il-Komunikazzjoni tal-Kummissjoni lill-Parlament Ewropew u lill-Kunsill: Inxejnu d-distakk tat-talent fiċ-ċibersigurtà biex nixprunaw il-kompetittività, it-tkabbir u r-reżiljenza tal-UE ("L-Akkademja tal-Ħiliet fiċ-Ċibersigurtà"). COM(2023) 207 final.

L-inkorporazzjoni tal-kompetenza diġitali u tal-moduli taċ-ċibersigurtà fil-kurrikuli edukattivi hi kruċjali biex iċ-ċibersigurtà fil-kura tas-saħħa tinbena fuq pedamenti sodi. Dawn il-moduli għandhom jindirizzaw ċerti kwistjonijiet speċifiċi għas-settur bħall-protezzjoni tad-data tal-pazjenti u l-vulnerabbiltajiet fis-sigurtà tal-apparati mediċi. L-iżvilupp ta' dawn ir-riżorsi għandu jqis l-azzjonijiet preċedenti, bħall-proġett BeWell iffinanzjat mill-programm Erasmus+[38] u l-proġett PANACEA ffinanzjat minn Orizzont 2020[39].

3.2. Kapaċitajiet Ewropej għall-identifikazzjoni ta' theddid ċibernetiku kontra s-settur tas-saħħa

Biex nipprovdu rispons fil-pront għall-inċidenti, importanti jkollna detezzjoni effettiva tat-theddid ċibernetiku. L-atturi tat-theddid jistgħu jużaw tekniki li jagħmluha diffiċli biex nidentifikaw l-intrużjonijiet tagħhom, u hekk ikollhom perjodi itwal ta' aċċess bla permess għas-sistemi[40]. Għaldaqstant, jekk intejbu l-kapaċitajiet tad-detezzjoni tat-theddid, dan jgħinna nwaqqfu l-attakki ċibernetiċi aktar kmieni. Pereżempju, fil-każ tal-attakk ransomware kontra l-fornitur Finlandiż tas-servizzi tal-psikoterapija Vastaamo, li matulu l-awtur estorċa lill-pazjenti li kienu nsterqulhom ir-rekords tas-saħħa tagħhom, l-intrużjoni inizjali kienet ġrat fl-2018, iżda l-fornitur induna biha biss fl-2020[41].

Il-kondiviżjoni effiċjenti tal-informazzjoni u l-kollaborazzjoni huma essenzjali biex titjieb id-detezzjoni tat-theddid u jiżdied l-għarfien sitwazzjonali madwar l-UE. L-Iskwadri tar-Rispons għal Inċidenti relatati mas-Sigurtà tal-Kompjuters (CSIRTs) jaqdu rwol vitali għax dawn jirċievu rapporti ta' inċidenti, kważi inċidenti u theddid potenzjali, u joffru gwida dwar il-miżuri tal-mitigazzjoni fil-livell nazzjonali. Iżda **l-Istati Membri huma mħeġġa ħafna biex maċ-Ċentru ta' Appoġġ tal-ENISA jaqsmu wkoll kull notifiki ta' inċident ċibernetiku li jirċievu mingħand l-isptarijiet u l-fornituri tal-kura tas-saħħa biex joktor l-għarfien sitwazzjonali tal-UE**. Idealment, dawn għandhom jiġu akkumpanjati b'dettalji sinifikattivi ta' diversi dimensjonijiet rilevanti tal-inċidenti, inkluż vulnerabbiltajiet ewlenin magħrufa u l-effetti fuq is-servizzi tal-kura tas-saħħa u l-avvenimenti negattivi għall-pazjenti. Barra minn hekk, il-manifatturi tal-apparati mediċi u dijanjostiċi *in vitro* huma mħeġġa jirrapportaw b'mod volontarju, fuq il-pjattaforma unika tar-rapportar li trid tistabbilixxi u tmexxi l-ENISA fil-qafas tal-Att dwar ir-Reżiljenza Ċibernetika, il-vulnerabbiltajiet sfruttati b'mod attiv jew l-inċidenti ċibernetiċi severi li jkollhom impatt fuq is-sigurtà ta' dawn l-apparati, kif ukoll vulnerabbiltajiet, inċidenti, kważi aċċidenti jew theddid ċibernetiku potenzjali ieħor li jista' jaffettwa l-profil tar-riskju ta' dawn l-apparati.

Meta l-informazzjoni fir-rapporti ma tkunx għadha sensittiva, iċ-Ċentru ta' Appoġġ jista' jibni katalogu Ewropew tal-vulnerabbiltajiet sfruttati magħrufa (KEV) sponsorjat mill-ENISA għall-apparati mediċi, is-sistemi tar-rekords elettroniċi tas-saħħa u għall-fornituri tat-tagħmir tal-ICT u tas-software fis-saħħa. Biex jiġu indirizzati ċerti sfidi sinifikanti tad-detezzjoni tat-theddid, iċ-Ċentru ta' Appoġġ għandu jintroduċi **servizz għas-settur tas-saħħa biex jabbonaw għal twissija bikrija madwar l-UE kollha li tibgħat twissijiet kważi fil-ħin reali**. Dan is-servizz jibbaża fuq id-data pproċessata mis-CSIRTs, l-entitajiet tal-kura tas-saħħa u l-manifatturi, l-Intelligence minn Sorsi Miftuħa (OSINT), u atturi rilevanti oħra bħaċ-Ċentri Ċibernetiċi, iċ-Ċentri tal-Kondiviżjoni u tal-Analiżi tal-Informazzjoni (ISACs) u l-awtoritajiet tal-infurzar tal-liġi. Il-kooperazzjoni msaħħa bejn l-ENISA u l-Aġenzija tal-Unjoni Ewropea għall-Kooperazzjoni fl-Infurzar tal-Liġi (Europol) –

---

38 BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills. https://bewell-project.eu/.

39 PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people. https://cordis.europa.eu/project/id/826293.

40 Ix-Xenarju tat-Theddid fl-2023 skont l-ENISA: is-Settur tas-Saħħa.

41 Id-Deċiżjoni 1150/161/2021 tal-Ombudsman Finlandiż għall-Protezzjoni tad-Data.

pereżempju dwar ix-xejriet taċ-ċiberkriminalità fis-settur tas-saħħa – tkompli tagħti spinta lill-għarfien sitwazzjonali.

L-ISACs huma riżorsi ċentrali għall-intelligence dwar it-theddid ċibernetiku, filwaqt li jrawmu l-kondiviżjoni tal-informazzjoni bidirezzjonali bejn is-settur pubbliku u privat, u jippromwovu l-bini tal-fiduċja. Iċ-Ċentru ta' Appoġġ għandu jżid l-appoġġ lill-**ISAC Ewropew tas-Saħħa** b'għodod u bi skambju tal-informazzjoni, b'rapporti dwar l-għarfien sitwazzjonali settorjali, kif ukoll billi jrawwem komunità fdata għal kollaborazzjoni tattika u strateġika. L-Istati Membri għandhom jinkoraġġixxu l-iżvilupp ta' ISACs nazzjonali tas-saħħa[42]. L-ISACs għandhom jitħeġġu wkoll ilaqqgħu flimkien lill-fornituri tal-kura tas-saħħa mal-manifatturi biex jinkiseb fehim konġunt tat-theddid ċibernetiku, inkluż fil-katina tal-provvista, u jiffaċilitaw djalogu dwar id-disinn sigur tal-prodotti li verament iqisu r-realtajiet tal-użu fil-prattika.

3.3. Rispons malajr u rkupru

Minħabba s-sensittività kbira tad-data dwar is-saħħa tal-pazjenti u l-effetti potenzjalment devastanti tal-attakki ċibernetiċi fuq is-servizzi tal-kura tas-saħħa, hu kruċjali li jsir rispons malajr u effettiv għall-inċidenti taċ-ċibersigurtà biex inħarsu s-sikurezza tal-pazjenti. Meta sptar jew fornitur tal-kura tas-saħħa jiffaċċja attakk ċibernetiku, l-ewwel punt tal-kuntatt hu s-CSIRT nazzjonali rilevanti[43]. Is-CSIRT hija responsabbli biex tipprovdi appoġġ fil-ħin, idealment fi żmien 24 siegħa, biex tgħin fil-ġestjoni tal-inċidenti sinifikanti. Iżda jekk inċident jaqbeż il-kapaċità tas-CSIRT, għandu jkun hemm l-appoġġ tal-UE biex ikun żgurat rispons malajr u effettiv.

Ir-Riżerva taċ-Ċibersigurtà tal-UE, stabbilita skont l-Att dwar iċ-Ċibersolidarjetà, tipprovdi servizzi ta' rispons għall-inċidenti mill-fornituri tas-sigurtà ġestiti fdati biex jassistu fl-inċidenti taċ-ċibersigurtà sinifikanti jew fuq skala kbira u matul l-isforzi inizjali tal-irkupru. Din ir-riżerva tfasslet biex tikkumplementa l-isforzi tas-CSIRTs tal-Istati Membri, u tippermettilhom jitolbu appoġġ addizzjonali fil-każijiet li jinvolvu setturi kritiċi bħas-saħħa. Biex isaħħu din is-sistema, il-**Kummissjoni u l-ENISA għandhom jiżguraw li r-Riżerva tkun tinkludi Servizz ta' Rispons Malajr b'mod speċifiku għas-settur tas-saħħa**. B'kumplimentarjetà ma' oqfsa eżistenti oħra, meta l-appoġġ nazzjonali ma jkunx biżżejjed, dan is-servizz ikun jista' jqabbad esperti biex jimmaniġġjaw mingħajr dewmien l-inċidenti taċ-ċibersigurtà sinifikanti jew fuq skala kbira fil-kura tas-saħħa.

Biex itejjeb ir-rispons u l-irkupru, iċ-Ċentru ta' Appoġġ, b'kollaborazzjoni mal-Grupp ta' Kooperazzjoni tan-NIS, man-Network tas-CSIRTs u, meta rilevanti, mal-Europol, għandu jiżviluppa **playbooks tar-rispons għall-inċidenti ċibernetiċi mfassla apposta għall-kura tas-saħħa**. Dawn il-playbooks jiggwidaw lis-CSIRTs u lill-organizzazzjonijiet tal-kura tas-saħħa fir-rispons għal theddid speċifiku taċ-ċibersigurtà, inkluż ir-ransomware. Minħabba l-importanza ta' kooperazzjoni effettiva fost is-CSIRTs u l-awtoritajiet tal-infurzar tal-liġi fir-rispons għall-inċidenti taċ-ċibersigurtà ta' natura kriminali u fl-investigazzjoni tagħhom, il-playbooks, fost aspetti oħra, għandhom jipprovdu gwida ċara għar-rapportar ta' dawn l-inċidenti lill-infurzar tal-liġi. Barra minn hekk, iċ-Ċentru ta' Appoġġ jista' **jiffaċilita l-introduzzjoni wiesgħa ta' eżerċizzji nazzjonali taċ-ċibersigurtà, u jibni fuq l-esperjenzi ta' eżerċizzji bħas-Cyber Europe 2022 tal-ENISA, biex jittestja l-playbooks u jsaħħaħ il-protokolli tar-rispons għall-inċidenti**.

---

42 Pereżempju, il-Finlandja għandha ISAC nazzjonali għas-settur tal-assistenza soċjali u l-kura tas-saħħa. Ara ċ-Ċentru Nazzjonali Finlandiż taċ-Ċibersigurtà: ISAC information sharing groups, żur https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

43 L-Artikolu 23(1) tad-Direttiva NIS 2 jistabbilixxi rekwiżit għall-entitajiet essenzjali u importanti biex jinnotifikaw inċidenti sinifikanti lis-CSIRT rilevanti jew, meta applikabbli, lill-awtorità kompetenti.

Biex il-politiki jiġu infurmati u tiġi vvalutata l-effettività tal-miżuri meħuda kontra l-attakki ransomware, jeħtieġ tinġabar aktar data. Għal dan il-għan, l-Istati Membri għandhom jitolbu lill-entitajiet soġġetti għad-Direttiva NIS 2, inkluż lill-organizzazzjonijiet tal-kura tas-saħħa, biex jirrapportaw dwar kull pagament ta' riskatt li jkun sar u dwar il-pagamenti tar-riskatt li jkun beħsiebhom jagħmlu, flimkien ma' informazzjoni oħra li jipprovdu meta jirrapportaw dwar inċidenti sinifikanti taċ-ċibersigurtà. Dan ir-rapportar jappoġġa l-investigazzjoni effettiva tal-inċidenti tar-ransomware, inkluż it-traċċar tal-pagamenti fuq il-pjattaformi tal-iskambju tal-kriptovaluti biex jiġu identifikati r-riċevituri.

Il-veloċità tal-irkupru hi fattur kritiku biex tissokta r-reżiljenza u l-fiduċja tal-pubbliku, b'mod partikolari fil-kura tas-saħħa, fejn il-ħinijiet tal-waqfien jistgħu jfixklu l-kura tal-pazjenti. Għal irkupru effettiv mill-attakki ransomware, il-fornituri tal-kura tas-saħħa jrid ikollhom backups siguri, aġġornati u iżolati li jistgħu jitreġġgħu lura malajr. Bħala parti mill-katalogu tas-servizzi tiegħu, iċ-Ċentru ta' Appoġġ jista' joffri **servizz ta' abbonament għall-irkupru tar-ransomware, li jgħin lill-isptarijiet u lill-fornituri tal-kura tas-saħħa jħejju pjanijiet tal-irkupru minn qabel**. L-ENISA u l-Europol għandhom jikkollaboraw flimkien biex jidentifikaw l-aktar xejriet komuni tar-ransomware immirati lejn l-organizzazzjonijiet tal-kura tas-saħħa u **jespandu r-repożitorju tal-għodod tad-dekriptaġġ** disponibbli permezz tal-proġett No More Ransom[44]. Għandhom jiżviluppaw u jippromwovu wkoll gwida aċċessibbli biex jgħinu lill-fornituri tal-kura tas-saħħa jevitaw li jħallsu riskatti billi jużaw għodod tad-dekriptaġġ.

L-**Inizjattiva Internazzjonali Kontra r-Ransomware**[45] hi lok siewi għall-iskambju dwar inċidenti speċifiċi tar-ransomware, kif ukoll biex jinbnew il-kapaċitajiet tal-pajjiżi membri ħalli jsaħħu l-oqfsa taċ-ċibersigurtà u l-kapaċitajiet tal-investigazzjoni tagħhom kontra l-atturi tar-ransomware. Il-Kummissjoni, id f'id mar-Rappreżentant Għoli, se tkompli tavvanza l-kooperazzjoni fl-Inizjattiva Kontra r-Ransomware, inkluż kontra t-theddid tar-ransomware għas-settur tas-saħħa. Barra minn hekk, il-Kummissjoni se tfittex kooperazzjoni fil-**Grupp ta' Ħidma tal-G7 dwar iċ-Ċibersigurtà** biex issaħħaħ iċ-ċibersigurtà tas-settur tas-saħħa. B'mod partikolari, il-Grupp ta' Ħidma jista' jikkunsidra possibbiltajiet biex is-settur tas-saħħa jiġi appoġġat kontra theddid bħar-ransomware, filwaqt li jibni fuq riflessjonijiet bħad-Dikjarazzjoni Konġunta dwar Attakki ta' Ransomware Kontra l-Faċilitajiet tal-Kura tas-Saħħa tat-8 ta' Novembru 2024 ippreżentata fil-kuntest tal-Kunsill tas-Sigurtà tan-Nazzjonijiet Uniti[46].

4. Azzjonijiet Nazzjonali

Il-kapaċità li dan il-Pjan ta' Azzjoni jtejjeb iċ-ċibersigurtà fis-settur tas-saħħa tiddependi fuq l-involviment attiv u l-impenn tal-Istati Membri. Biex il-Pjan ta' Azzjoni jimplimentawh b'suċċess, l-Istati Membri jistgħu jistabbilixxu **Ċentri Nazzjonali ta' Appoġġ għaċ-Ċibersigurtà speċifikament għall-isptarijiet u l-fornituri tal-kura tas-saħħa**. Dawn iċ-ċentri jaġixxu bħala l-punti primarji tal-kuntatt għas-settur tas-saħħa fil-livell nazzjonali, u jikkollaboraw mill-qrib maċ-Ċentru ta' Appoġġ tal-ENISA. Meta possibbli u rilevanti, l-Istati Membri għandhom jaħtru lil korpi eżistenti, bħas-CSIRTs nazzjonali tas-saħħa jew lill-awtoritajiet rilevanti, bħala Ċentri Nazzjonali ta' Appoġġ għaċ-Ċibersigurtà.

L-Istati Membri qed jitħeġġu wkoll joħolqu **pjanijiet ta' azzjoni nazzjonali ffukati fuq iċ-ċibersigurtà fis-settur tas-saħħa**. Dawn il-pjanijiet jiddeskrivu r-riskji speċifiċi għaċ-ċibersigurtà

---

44 https://www.nomoreransom.org/en/index.html.

45 https://www.counter-ransomware.org/

46 https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/

ffaċċjati mis-sistemi tal-kura tas-saħħa u l-azzjonijiet nazzjonali li qed jittieħdu biex jindirizzawhom, filwaqt li jiżguraw ukoll li r-riżorsi u l-prattiki fil-livell Ewropew jintużaw b'mod effettiv. Iċ-Ċentru ta' Appoġġ tal-ENISA jista' jassisti fl-iżvilupp ta' dawn il-pjanijiet, filwaqt li jqis il-pjanijiet nazzjonali diġà eżistenti u jikkoordina l-isforzi biex jiżgura li r-riżorsi u l-istrateġiji tal-Istati Membri individwali jkunu jikkumplimentaw lil xulxin.

L-Istati Membri jeħtieġ jixħtu enfasi partikolari fuq li jiffaċilitaw il-kondiviżjoni tar-riżorsi bejn il-fornituri tal-kura tas-saħħa, u dan jistgħu jiksbuh bl-**akkwist konġunt jew bl-akkomunament tar-riżorsi** fil-livell nazzjonali, reġjonali, jew anki Ewropew. Dan l-approċċ inaqqas il-piż finanzjarju fuq l-entitajiet individwali filwaqt li jżidilhom is-setgħa tan-negozjar mal-fornituri tas-servizzi taċ-ċibersigurtà.

Ngħidu aħna, il-programm Franċiż CaRE[47] introduċa għadd ta' miżuri fil-livell nazzjonali u reġjonali biex jiġu indirizzati ċerti sfidi fir-riżorsi: katalogu ċibernetiku jagħti ħarsa ġenerali lejn is-soluzzjonijiet u l-pakketti ċibernetiċi disponibbli għall-isptarijiet mill-aġenzija nazzjonali taċ-ċibersigurtà, l-aġenzija tas-saħħa diġitali, l-aġenziji reġjonali, l-organizzazzjonijiet nazzjonali tax-xiri, kif ukoll soluzzjonijiet kummerċjali. Dan hu kkumplimentat b'finanzjament addizzjonali għall-aġenziji reġjonali biex joffru riżorsi kondiviżi.

L-Istati Membri għandhom jindirizzaw ukoll il-livelli insuffiċjenti ta' investiment fiċ-ċibersigurtà fis-settur tas-saħħa. Biex jiżguraw finanzjament adegwat, dawn għandhom jistabbilixxu **parametri referenzjarji mhux vinkolanti u jimmonitorjaw il-miri tal-finanzjament li jkunu maħsuba speċifikament għaċ-ċibersigurtà**, filwaqt li jiżguraw li dawn l-investimenti ma jnaqqsux mill-kura essenzjali tal-pazjenti. Dawn il-miri tal-finanzjament għandu jkollhom ukoll l-għan li jintegraw il-kunsiderazzjonijiet tas-sigurtà fl-investimenti diġitali kollha fis-settur. L-Istati Membri jistgħu jiskambjaw l-aqwa prattiki u pariri dwar dawn il-miri permezz ta' pjattaformi bħan-Network tas-Saħħa Elettronika[48].

5. Kooperazzjoni Pubblika Privata

Il-kooperazzjoni pubblika privata u l-konsultazzjoni mal-fornituri tal-kura tas-saħħa, entitajiet oħra tas-settur tas-saħħa, kif ukoll l-atturi rilevanti tal-industrija taċ-ċibersigurtà, huma essenzjali għall-implimentazzjoni b'suċċess tal-Pjan ta' Azzjoni. Biex tkompli tikkontribwixxi għall-ħidma taċ-Ċentru ta' Appoġġ, **il-Kummissjoni, bl-appoġġ tal-ENISA, se tistabbilixxi Bord Konsultattiv taċ-Ċibersigurtà tas-Saħħa konġunt** b'rappreżentanti ta' livell għoli taż-żewġ oqsma, tal-kura tas-saħħa u taċ-ċibersigurtà, li jista' jagħti pariri lill-Kummissjoni u liċ-Ċentru ta' Appoġġ dwar azzjonijiet li jħallu impatt u jiddiskuti l-iżvilupp ulterjuri ta' sħubijiet pubbliċi privati f'dan il-qasam. Il-Bord se jibni fuq l-isforzi eżistenti għal sħubijiet pubbliċi privati, inkluż l-ISAC tas-Saħħa Ewropea.

Barra minn hekk, il-Kummissjoni se tniedi **sejħa għal azzjoni** biex il-kumpaniji taċ-ċibersigurtà, il-fondazzjonijiet, l-istituzzjonijiet edukattivi, u l-partijiet ikkonċernati tal-industrija **jwiegħdu azzjonijiet li jindirizzaw l-isfidi fis-settur**. Filwaqt li jibnu fuq l-esperjenza tal-Akkademja tal-Ħiliet fiċ-Ċibersigurtà, dawk l-impenji jistgħu jkunu pereżempju wegħdiet permezz tal-Akkademja tal-Ħiliet fiċ-Ċibersigurtà li jinkludu l-forniment ta' korsijiet u materjali tat-taħriġ b'enfasi fuq is-settur tas-saħħa għall-professjonisti taċ-ċibersigurtà[49]. Impenji oħra jistgħu jindirizzaw ukoll l-attivitajiet li

[47] L-Aġenzija Franċiża tas-Saħħa Diġitali: Cybersécurité acceleration et Résilience des Établissements (CaRE). https://esante.gouv.fr/strategie-nationale/cybersecurite.

[48] In-Network tas-saħħa elettronika hu network volontarju ta' awtoritajiet nazzjonali responsabbli għas-saħħa elettronika maħtura mill-Istati Membri u hu stabbilit skont l-Artikolu 14 tad-Direttiva 2011/24/UE.

[49] Cyber Skills Academy: Get Involved | Digital Skills and Jobs Platform

jxerrdu l-għarfien jew il-forniment bla ħlas jew bi prezz ridott ta' servizzi tas-sigurtà ġestiti lil ċerti entitajiet speċifikament vulnerabbli biex iżidu t-tħejjija u r-reżiljenza tagħhom taċ-ċibersigurtà. Barra minn hekk, l-impenji jistgħu jinkludu l-kondiviżjoni ta' intelligence dwar it-theddid ċibernetiku maċ-Ċentru ta' Appoġġ tal-ENISA. Iċ-Ċentru ta' Appoġġ għandu jżomm ħarsa ġenerali tal-wegħdiet li jkunu saru fis-sejħa għal azzjoni, biex jiżgura l-koerenza u l-kumplimentarjetà tagħhom.

6. Skoraġġiment tal-atturi tat-theddid ċibernetiku

Il-politiki interni u esterni tal-UE dwar iċ-ċibersigurtà għandhom jappoġġaw l-għan li l-atturi tat-theddid ċibernetiku jiġu skoraġġuti milli jattakkaw is-sistemi tal-kura tas-saħħa Ewropej. L-attakki ċibernetiċi kontra l-organizzazzjonijiet tal-kura tas-saħħa huma tip partikolarment inaċċettabbli ta' attività ċibermalizzjuża, minħabba l-kapaċità tagħhom li jheddu s-sikurezza tal-pazjenti u ħajjet in-nies. Għalhekk, il-forza sħiħa tal-kapaċitajiet tal-iskoraġġiment tal-UE fil-qasam taċ-ċibersigurtà u tal-infurzar tal-liġi għandha tintuża biex iddgħajjef il-mudell kummerċjali ġenerali tal-atturi tat-theddid immirat lejn is-settur tas-saħħa, u biex iċċaħħadhom minn profitti faċli. Dan jinkludi li jitrawmu investigazzjonijiet transfruntieri b'kondiviżjoni msaħħa tal-indikaturi ta' kompromess u data rilevanti oħra, u enfasi akbar fuq il-miri ta' valur għoli u l-faċilitaturi kriminali ewlenin bħal webhosting insuperabbli jew servizzi tat-taħlit tal-kriptovaluti.

Is-**Sett ta' Għodod taċ-Ċiberdiplomazija** joffri qafas għall-prevenzjoni, l-iskoraġġiment u r-rispons għall-attakki ċibernetiċi kontra l-UE, l-Istati Membri u s-sħab. Ir-Rappreżentant Għoli se jkompli juża l-qafas eżistenti tas-sanzjonijiet ċibernetiċi biex iwieġeb għat-theddid immirat lejn is-sistemi tas-saħħa.

Forma ta' skoraġġiment importanti hi li l-atturi kriminali jinżammu responsabbli għall-azzjonijiet tagħhom. Għalhekk, l-Istati Membri għandhom jiżguraw li l-infurzar tal-liġi jkun integrat għalkollox fil-pjanijiet ta' azzjoni nazzjonali tagħhom. B'mod partikolari, għandhom iħaddmu bis-sħiħ id-dispożizzjonijiet tad-Direttiva dwar l-attakki fuq is-sistemi tal-informazzjoni[50] u tal-Konvenzjoni ta' Budapest tal-Kunsill tal-Ewropa dwar iċ-Ċiberkriminalità biex jiskoraġġixxu l-attakki, iressqu lill-kriminali quddiem il-ġustizzja u jżarmaw l-infrastrutturi kriminali li jiffaċilitaw l-attakki[51]. L-implimentazzjoni b'suċċess ta' dawn l-għodod għandha tiżgura l-kastig għall-azzjonijiet kriminali u malizzjużi kontra l-kura tas-saħħa.

7. Implimentazzjoni u monitoraġġ tal-Pjan ta' Azzjoni

Tul dan il-Pjan ta' Azzjoni, ġew previsti għadd ta' kompiti biex jiġi stabbilit Ċentru ta' Appoġġ fi ħdan l-ENISA. Dan jiżgura implimentazzjoni ħolistika u koerenti tal-Pjan ta' Azzjoni filwaqt li jevita l-ħolqien ta' entitajiet ġodda li jwasslu għal dupplikazzjonijiet potenzjali u aktar spejjeż. Il-Kummissjoni beħsiebha tiżgura li ċ-Ċentru ta' Appoġġ ikollu r-riżorsi meħtieġa.

Ladarba ċ-Ċentru ta' Appoġġ ikun jista' jibda jitħaddem, l-ENISA, b'konsultazzjoni mal-Kummissjoni, għandha tipprovdi aġġornamenti regolari tal-ħidma taċ-Ċentru ta' Appoġġ lill-Bord tat-Tmexxija tal-ENISA kif ukoll lin-networks rilevanti tal-Istati Membri, b'mod partikolari lill-Grupp ta' Kooperazzjoni tal-NIS, lin-Network tas-CSIRTs, lin-Network tas-saħħa elettronika u meta

50 Id-Direttiva 2013/40/UE tal-Parlament Ewropew u tal-Kunsill tat-12 ta' Awwissu 2013 dwar attakki kontra s-sistemi tal-informazzjoni u li tissostitwixxi d-Deċiżjoni Qafas tal-Kunsill 2005/222/ĠAI: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng

51 Il-Konvenzjoni dwar iċ-Ċiberkriminalità (il-Konvenzjoni ta' Budapest, ETS Nru 185) u l-Protokolli tagħha: https://www.coe.int/en/web/cybercrime/the-budapest-convention

rilevanti, lill-Bord tal-Ispazju Ewropew tad-Data dwar is-Saħħa. Barra minn hekk, l-ENISA għandha tiskambja kontinwament mal-Bord Konsultattiv pubbliku privat taċ-Ċibersigurtà tas-Saħħa dwar l-implimentazzjoni tal-azzjonijiet ipprovduti miċ-Ċentru ta' Appoġġ.

Ir-rapporti regolari tal-ENISA, bħar-Rapport dwar l-Istat taċ-Ċibersigurtà fl-Unjoni, li jipprovdi valutazzjoni aggregata tal-livell ta' maturità tal-kapaċitajiet u r-riżorsi taċ-ċibersigurtà madwar l-UE, inkluż fis-settur tas-saħħa, għandhom ikunu okkażjonijiet biex tiġi ppubblikata data rilevanti, li tappoġġa l-monitoraġġ tal-Pjan ta' Azzjoni. Barra minn hekk, l-Indiċi taċ-Ċibersigurtà tal-UE tal-ENISA[52] jista' jipprovdi data kwantitattiva u kwalitattiva, li tkun bażi tal-evidenza għall-valutazzjoni tal-kritikalità u tal-maturità tas-settur tas-saħħa.

8. Passi li jmiss

Din il-Komunikazzjoni stabbiliet aġenda ambizzjuża biex l-UE jkollha settur tas-saħħa aktar ċibersigur. Bl-iżvilupp propost taċ-Ċentru ta' Appoġġ għaċ-Ċibersigurtà għall-Isptarijiet u l-Fornituri tal-Kura tas-Saħħa fil-qalba tal-ENISA, il-Pjan ta' Azzjoni jistabbilixxi triq biex jissawwar approċċ Ewropew koerenti u komuni għall-isfida taċ-ċibersigurtà fis-settur.

Din il-Komunikazzjoni għandha titqies bħala l-bidu ta' proċess biex tittejjeb iċ-ċibersigurtà fis-settur tas-saħħa. Għalhekk, apparti l-adozzjoni tal-Pjan ta' Azzjoni, se jitnedew konsultazzjonijiet komprensivi mal-partijiet ikkonċernati u jissoktaw l-iskambji mal-Istati Membri u n-networks rilevanti biex jinġabar l-għarfien. Abbażi tar-riżultati tal-konsultazzjonijiet, il-Kummissjoni beħsiebha tressaq rakkomandazzjonijiet fir-raba' kwart tal-2025 biex tkompli tirfina l-Pjan ta' Azzjoni.

Il-Kummissjoni tappella lill-Istati Membri u lill-partijiet ikkonċernati kollha biex jaħdmu flimkien fit-twettiq tal-ambizzjoni tal-Pjan ta' Azzjoni.

[52] L-ENISA, EU Cybersecurity Index, Framework and Methodological Note (2024). https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

ANNESS

Ħarsa ġenerali lejn l-azzjonijiet proposti

Il-Kummissjoni:

iċ-Ċentru ta' Appoġġ għaċ-Ċibersigurtà tal-ENISA għall-Isptarijiet u l-Fornituri tal-Kura tas-Saħħa	
Niżguraw ir-riżorsi xierqa għaċ-Ċentru ta' Appoġġ għaċ-Ċibersigurtà Ħidma mal-ECCC biex jitnedew proġetti pilota li jiżviluppaw l-aqwa prattiki għaċ-ċiberiġjene u l-valutazzjoni tar-riskji għas-sigurtà, u biex tiġi indirizzata l-ħtieġa ta' monitoraġġ kontinwu taċ-ċibersigurtà, intelligence dwar it-theddid u r-rispons għall-inċidenti b'soluzzjonijiet taċ-ċibersigurtà mill-aktar avvanzati, biex jinkiseb katalogu tas-servizzi taċ-Ċentru Ewropew ta' Appoġġ fil-qasam taċ-ċibersigurtà	2025
Prevenzjoni tal-inċidenti taċ-ċibersigurtà	
B'konsultazzjoni mal-Grupp ta' Kooperazzjoni tan-NIS, l-EU-CyCLONe u l-ENISA, is-saħħa possibbilment tiġi identifikata bħala settur li għalih jista' jingħata appoġġ għall-ittestjar ikkoordinat tat-tħejjija skont l-Att dwar iċ-Ċibersolidarjetà	Q1 2025
Rispons malajr u rkupru	
Flimkien mal-ENISA, ikun żgurat li r-Riżerva taċ-Ċibersigurtà tal-UE tkun tinkludi Servizz ta' Rispons Rapidu speċifikament għas-settur tas-saħħa	Q4 2025
Kooperazzjoni Pubblika Privata	
Bl-appoġġ tal-ENISA, jitwaqqaf Bord Konsultattiv konġunt taċ-Ċibersigurtà tas-Saħħa	Q1 2025
Titnieda sejħa għal azzjoni biex il-kumpaniji taċ-ċibersigurtà, il-fondazzjonijiet, l-istituzzjonijiet edukattivi, u l-partijiet ikkonċernati tal-industrija jwiegħdu azzjonijiet li jindirizzaw l-isfidi fis-settur tas-saħħa	Q2 2025
Skoraġġiment tal-atturi tat-theddid ċibernetiku	
Flimkien mar-Rappreżentant Għoli, jiġi esplorat l-użu ta' miżuri mis-Sett tal-Għodod taċ-Ċiberdiplomazija għall-prevenzjoni, l-iskoraġġiment u r-rispons għall-attivitajiet malizzjużi kontra s-sistemi tas-saħħa	2025
Jissokta l-avvanz fil-kooperazzjoni internazzjonali kontra l-atturi tar-ransomware, b'mod partikolari fl-Inizjattiva Internazzjonali Kontra r-Ransomware, id f'id mar-Rappreżentant Għoli	2025-2026
Issir ħidma favur kooperazzjoni fil-Grupp ta' Ħidma tal-G7 dwar iċ-Ċibersigurtà biex tissaħħaħ iċ-ċibersigurtà tas-settur tas-saħħa	2025-2026
Passi li jmiss	
Jitnedew konsultazzjonijiet komprensivi mal-partijiet ikkonċernati	Q1 2025
Jiġu adottati rakkomandazzjonijiet li jkomplu jirfinaw il-Pjan ta' Azzjoni	Q4 2025

L-ENISA:

iċ-Ċentru ta' Appoġġ tal-UE għaċ-Ċibersigurtà għall-Isptarijiet u l-Fornituri tal-Kura tas-Saħħa	
Tibda l-ħidma biex jiġi stabbilit Ċentru Ewropew ta' Appoġġ għaċ-Ċibersigurtà għall-isptarijiet u l-fornituri tal-kura tas-saħħa	Q2 2025
Jinħoloq katalogu tas-servizzi komprensivi li jrid jipprovdi ċ-Ċentru ta' Appoġġ għaċ-Ċibersigurtà	Minn Q4 2025
Prevenzjoni tal-inċidenti taċ-ċibersigurtà	
Tinħareġ gwida li tenfasizza l-aktar prattiki kritiċi taċ-ċibersigurtà u tgħin lill-fornituri tal-kura tas-saħħa fl-implimentazzjoni tagħhom	Q3 2025
B'kollaborazzjoni mill-qrib mal-Kummissjoni u mal-Istati Membri, tinħoloq għodda għall-immappjar regolatorju	Q1 2025
Jinħoloq qafas għal valutazzjonijiet tal-maturità taċ-ċibersigurtà li jkunu speċifiċi għall-kura tas-saħħa	Q3 2025
Issir Valutazzjoni annwali tal-Maturità Ċibernetika tas-Saħħa	2025-2026
Issir kollaborazzjoni mal-Istati Membri u mal-awtoritajiet reġjonali tal-programmi biex jinħolqu programmi mudell għall-Vawċer taċ-Ċibersigurtà	2025-2026
Jinħolqu linji gwida ġodda dwar l-akkwist għaċ-ċibersigurtà tal-isptarijiet u l-fornituri tal-kura tas-saħħa	Q3 2025
Jiġi stabbilit Network Ewropew ta' CISOs tas-Saħħa	Q1 2026
Jitfasslu u ssir promozzjoni ta' moduli u korsijiet tat-taħriġ għall-professjonisti tal-kura tas-saħħa	Q1 2026
Kapaċitajiet Ewropej għall-identifikazzjoni ta' theddid ċibernetiku kontra s-settur tas-saħħa	
Jinħoloq katalogu Ewropew tal-KEV għall-apparati mediċi, is-sistemi tar-rekords elettroniċi tas-saħħa u l-fornituri tat-tagħmir u s-software tal-ICT fis-saħħa	Q4 2025
Jiddaħħal servizz ta' abbonament ta' twissija bikrija fl-UE kollha għas-settur tas-saħħa	Mill-2026
Jingħata appoġġ lill-ISAC tas-Saħħa Ewropea b'għodod u skambju tal-informazzjoni	2025-2026
Rispons malajr u rkupru	
Flimkien mal-Kummissjoni, ikun żgurat li r-Riżerva taċ-Ċibersigurtà tal-UE tkun tinkludi Servizz ta' Rispons Rapidu speċifikament għas-settur tas-saħħa	Q4 2025
B'kollaborazzjoni man-Network tas-CSIRTs, jinħolqu playbooks dwar ir-rispons għall-inċidenti ċibernetiċi li jkunu mfassla apposta għall-kura tas-saħħa	Q3 2025
Teħfief l-introduzzjoni wiesgħa ta' eżerċizzji nazzjonali taċ-ċibersigurtà biex jiġu ttestjati l-playbooks u jissaħħu l-protokolli tar-rispons għall-inċidenti	Minn Q4 2025
Jingħata servizz ta' abbonament għall-irkupru minn ransomware	Mill-2026
Flimkien mal-Europol, jingħarfu l-aktar xejriet komuni tar-ransomware mmirati lejn l-organizzazzjonijiet tal-kura tas-saħħa u jitwessa' r-repożitorju tal-għodod tad-dekriptaġġ permezz tal-proġett No More Ransom.	Q4 2025

Flimkien mal-Europol, tinħoloq gwida aċċessibbli biex tgħin lill-fornituri tal-kura tas-saħħa jevitaw li jħallsu r-riskatti	Q3 2025
Azzjonijiet Nazzjonali	
Tingħata assistenza lill-Istati Membri biex joħolqu l-pjanijiet ta' azzjoni nazzjonali	2025
Jiġu kkoordinati l-isforzi biex ikun żgurat li r-riżorsi u l-istrateġiji tal-Istati Membri individwali jkunu jikkumplimentaw lil xulxin	2025-2026
Implimentazzjoni u monitoraġġ tal-Pjan ta' Azzjoni	
B'konsultazzjoni mal-Kummissjoni, jingħataw aġġornamenti regolari dwar il-ħidma taċ-Ċentru ta' Appoġġ għaċ-Ċibersigurtà lin-networks rilevanti tal-Istati Membri	2025-2026
Isir skambju kontinwu mal-Bord Konsultattiv taċ-Ċibersigurtà tas-Saħħa	2025-2026

L-Istati Membri:

Kapaċitajiet Ewropej għall-identifikazzjoni ta' theddid ċibernetiku kontra s-settur tas-saħħa	
In-notifiki tal-inċidenti li jġarrbu l-isptarijiet u l-fornituri tal-kura tas-saħħa skont in-NIS 2 jiġu kondiviżi maċ-Ċentru Ewropew ta' Appoġġ għaċ-Ċibersigurtà	Minn Q4 2025
Jitħeġġeġ l-iżvilupp ta' ISACs nazzjonali tas-saħħa	2025-2026
Prevenzjoni tal-inċidenti taċ-ċibersigurtà	
Fi ħdan il-Grupp ta' Kooperazzjoni tal-NIS, issir valutazzjoni kkoordinata tar-riskji għas-sigurtà, li tivvaluta r-riskji tekniċi u anki strateġiċi relatati mal-ktajjen tal-provvista tal-apparati mediċi	Q4 2025
Rispons malajr u rkupru	
Jitnedew eżerċizzji nazzjonali taċ-ċibersigurtà biex jiġu ttestjati l-playbooks u jissaħħu l-protokolli tar-rispons għall-inċidenti	Mill-2026
Azzjonijiet Nazzjonali	
Jitwaqqfu ċ-Ċentri Nazzjonali ta' Appoġġ għaċ-Ċibersigurtà għall-isptarijiet u l-fornituri tal-kura tas-saħħa	Q2 2025
Jinħolqu pjanijiet ta' azzjoni nazzjonali ffukati fuq iċ-ċibersigurtà fis-settur tas-saħħa	Q4 2025
Teħfief il-kondiviżjoni tar-riżorsi fost il-fornituri tal-kura tas-saħħa	2025-2026
Jinħolqu parametri referenzjarji mhux vinkolanti u jsir monitoraġġ tal-miri tal-finanzjament li jkunu mmirati speċifikament għaċ-ċibersigurtà	Q4 2025
L-organizzazzjonijiet tal-kura tas-saħħa u entitajiet oħra soġġetti għad-Direttiva NIS 2 jintalbu jirrapportaw kull darba li jkun beħsiebhom iħallsu xi riskatti	Q4 2025