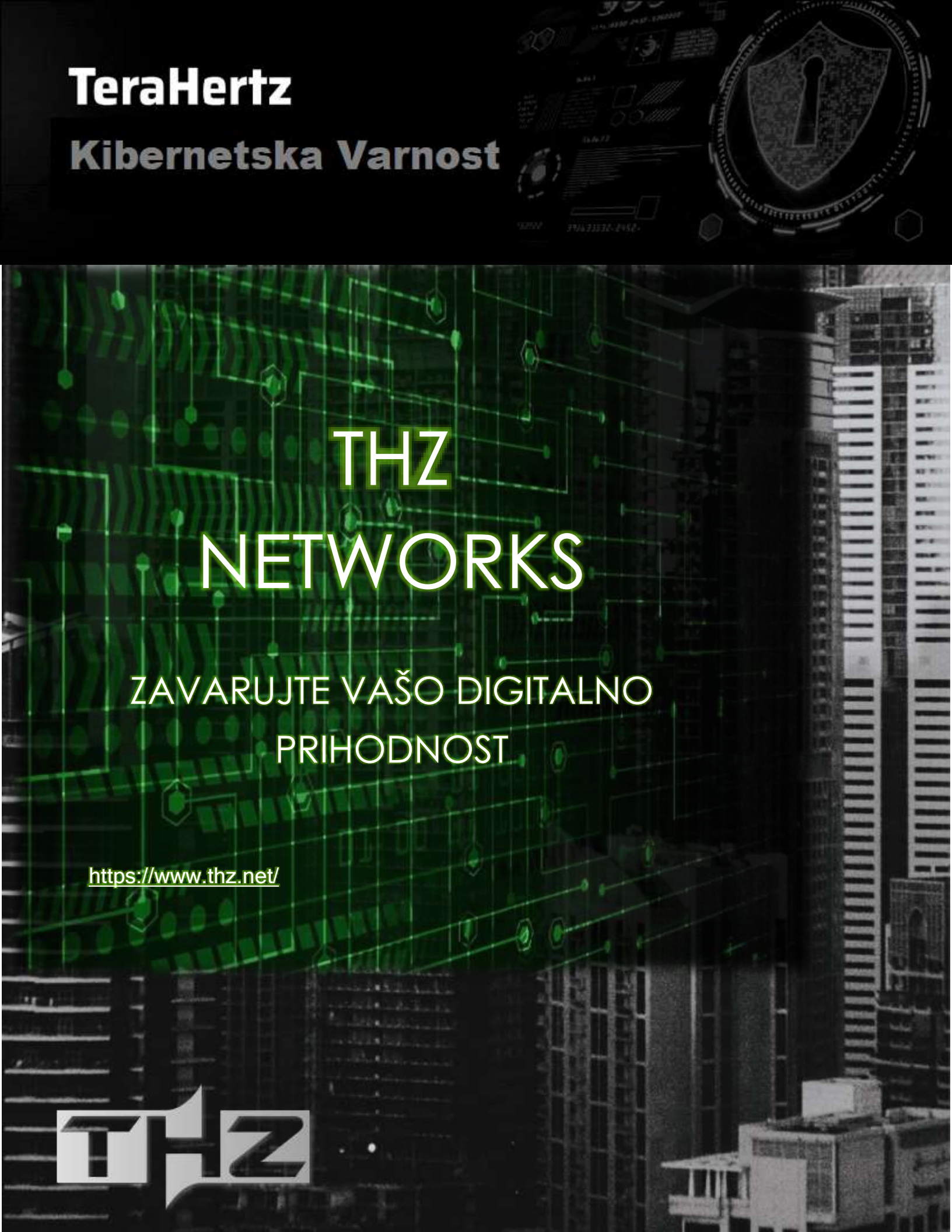
TeraHertz

Kibernetska Varnost



THZ NETWORKS

ZAVARUJTE VAŠO DIGITALNO PRIHODNOST

https://www.thz.net/

"Fas est et ab hoste doceri."

Publius Ovidius Naso, Metamorfoze, 8 n. št.

Pregled vsebine

THZ NETWORKS

Naša vizija

Naša vizija temelji na ustvarjanju varnega digitalnega okolja, kjer lahko posamezniki in podjetja brezkrbno poslujejo in sodelujejo.

Kot podjetje, ki ceni osebni pristop, zanesljivost in strast do kibernetske varnosti, se osredotočamo na gradnjo močnih odnosov z našimi strankami ter zagotavljanje vrhunskih storitev.

S strokovnim znanjem in našo inovativnostjo skupaj ustvarjamo varnostne rešitve, ki omogočajo trajnostno rast in zaupanje v digitalno prihodnost.

Miha Lavrič
CTO

O nas

THZ ekipo sestavlja skupina strokovnjakov kibernetske varnosti z izkušnjami iz različnih sektorjev področij dela (vladne službe, policija, pravo, analitika ipd.) v Varnostno operativnem centru (ang. SOC) in njihov vodja. S tem omogočamo 24/7 pokritost.

Našo zanesljivost in strokovnost potrjuje sodelovanje z več kot 15 podjetji iz sektorja kritične infrastrukture in zasebnega sektorja, ki skupaj zaposlujejo več tisoč ljudi.

Gre za visoko usposobljeno skupino s certifikati, ki pričajo o strokovnem znanju v kibernetski varnosti v širšem pomenu in poznavanju regulativnih okvirov, kot so:

- **PCI DSS**
- **HIPAA**
- **AICPA/SOC**
- **GDPR**
- **ISO 27001**
- **ISO 9003**
- **NIST**
- **NIS 2**

Pomen kibernetske varnosti

Zakaj je kibernetska varnost pomembna?

Kibernetska varnost je ključna za zaščito občutljivih podatkov, zagotavljanje nemotenega delovanja sistemov in preprečevanje kibernetskih napadov, ki lahko povzročijo resne motnje ali škodo. Zaradi vse večje digitalizacije in povezljivosti sistemov, kibernetska varnost postaja osrednji element za:

- Preprečevanje nepooblaščenega dostopa,
- zaščito pred motnjami,
- ohranjanje zaupanja,
- varstvo osebnih in finančnih podatkov in
- odziv na nove grožnje.

Vpliv na državni sektor, kritično infrastrukturo in poslovni sektor

Kibernetska varnost vpliva na delovanje vseh sektorjev kritične infrastrukture, državnih organov in poslovnega sektorja (vključno z bančnim sistemom, zavarovalnicami in velikimi podjetji) na naslednje načine:

- Zaščita pred kibernetskimi napadi,
- ohranjanje nemotenega delovanja,
- zmanjšanje gospodarske in finančne škode,
- podpora poslovnemu kontinuumu,
- skladnost z zakonodajo in
- odziv na nove grožnje.

KIBERNETSKA ZAŠČITA JE KLJUČNA

Kritična infrastruktura, finančne institucije in velika podjetja so pogosto tarča sofisticiranih kibernetskih napadov, ki lahko povzročijo motnje v oskrbi z energijo, vodo, zdravstvenimi storitvami, finančnimi storitvami in drugimi ključnimi storitvami.

Če so informacijski sistemi državnih organov, finančnih institucij ali velikih podjetij izpostavljeni napadom, lahko to vodi v paralizo ključnih funkcij, kot so nacionalna obramba, javna varnost, finančne transakcije ali dobavne verige. Kibernetska varnost pomaga preprečiti take scenarije.

Direktiva NIS 2 in korelacija kibernetske varnosti v državnem sektorju, kritični infrastrukturi in poslovnem sektorju

Direktiva NIS2 je posodobljena različica izvirne direktive o varnosti omrežij in informacij, katere cilj je izboljšati položaj kibernetske varnosti v Evropski uniji (EU). Neposredno je povezana s kibernetsko varnostjo, saj določa višje standarde in širi obseg subjektov, ki se morajo držati strogih ukrepov kibernetske varnosti.

To vključuje kritične sektorje, kot so: energetika, promet, bančništvo, zdravstvo in digitalna infrastruktura, pa tudi javnea uprava in srednja podjetja. Direktiva določa, da morajo ti subjekti izvajati stroge ukrepe za kibernetsko varnost, izvajati redne ocene tveganja in poročati o pomembnih incidentih nacionalnim organom.

POMEN DIREKTIVE NIS 2

Z uvedbo se želi povečati odpornost digitalne infrastrukture EU, zmanjšati tveganje kibernetskih napadov in izboljšati splošno okolje kibernetske varnosti v državah članicah. Ta usklajen pristop pomaga zmanjšati neskladja v praksah kibernetske varnosti v različnih državah, kar spodbuja varnejši in enotnejši digitalni trg.

Koristi za države članice EU vključujejo večjo zaščito kritične infrastrukture, boljše sodelovanje in izmenjavo informacij med državami članicami ter močnejšo kolektivno obrambo pred kibernetskimi grožnjami.

Direktiva tudi zagotavlja, da so države članice bolje pripravljene na odzivanje na incidente, s čimer se čim bolj zmanjša vpliv kibernetskih napadov na njihova gospodarstva in družbe. V Sloveniji bo NIS 2 urejena z Zakonom o informacijski varnosti (ZInfV-1)

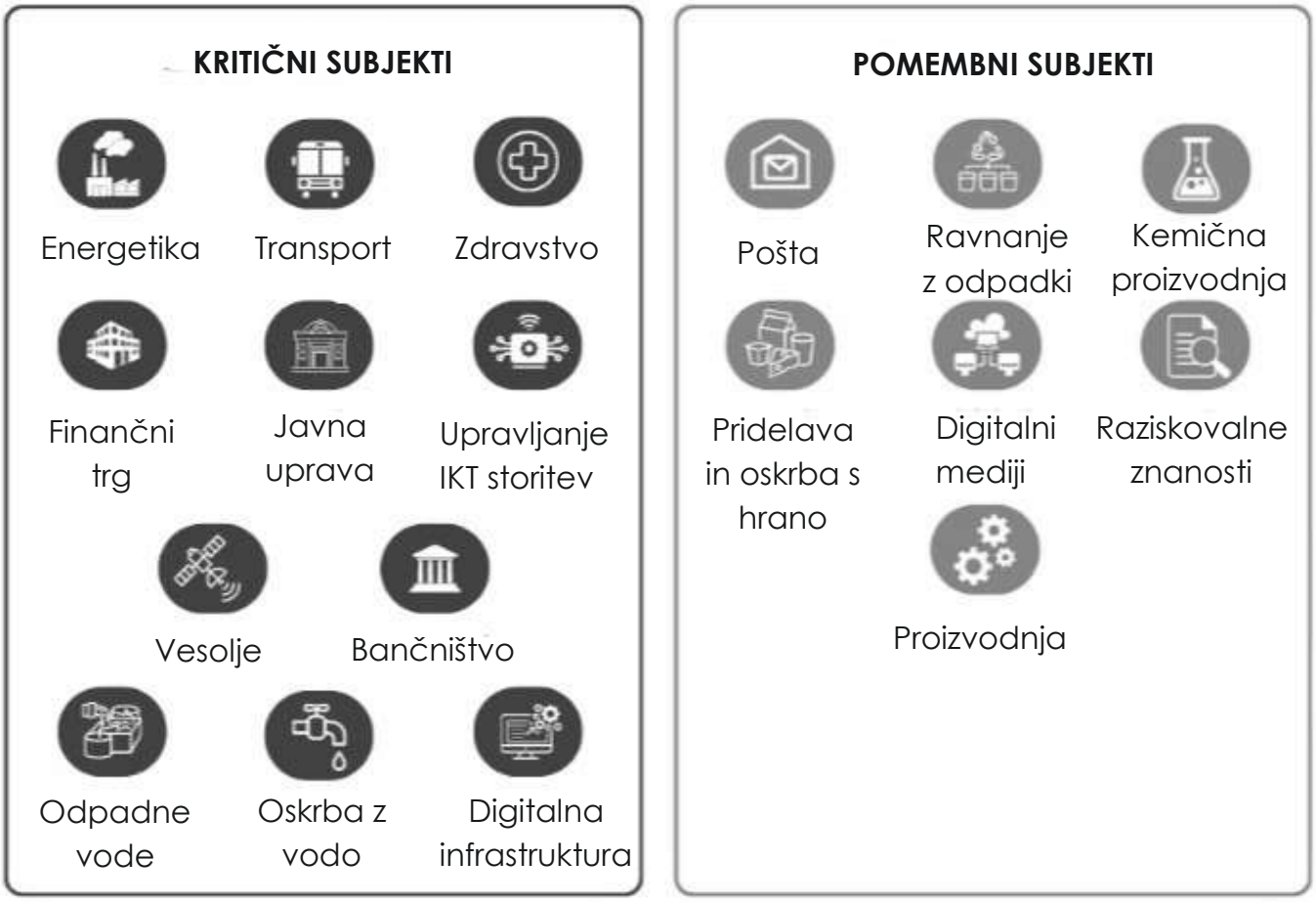
Delitev na bistvene in pomembne subjekte

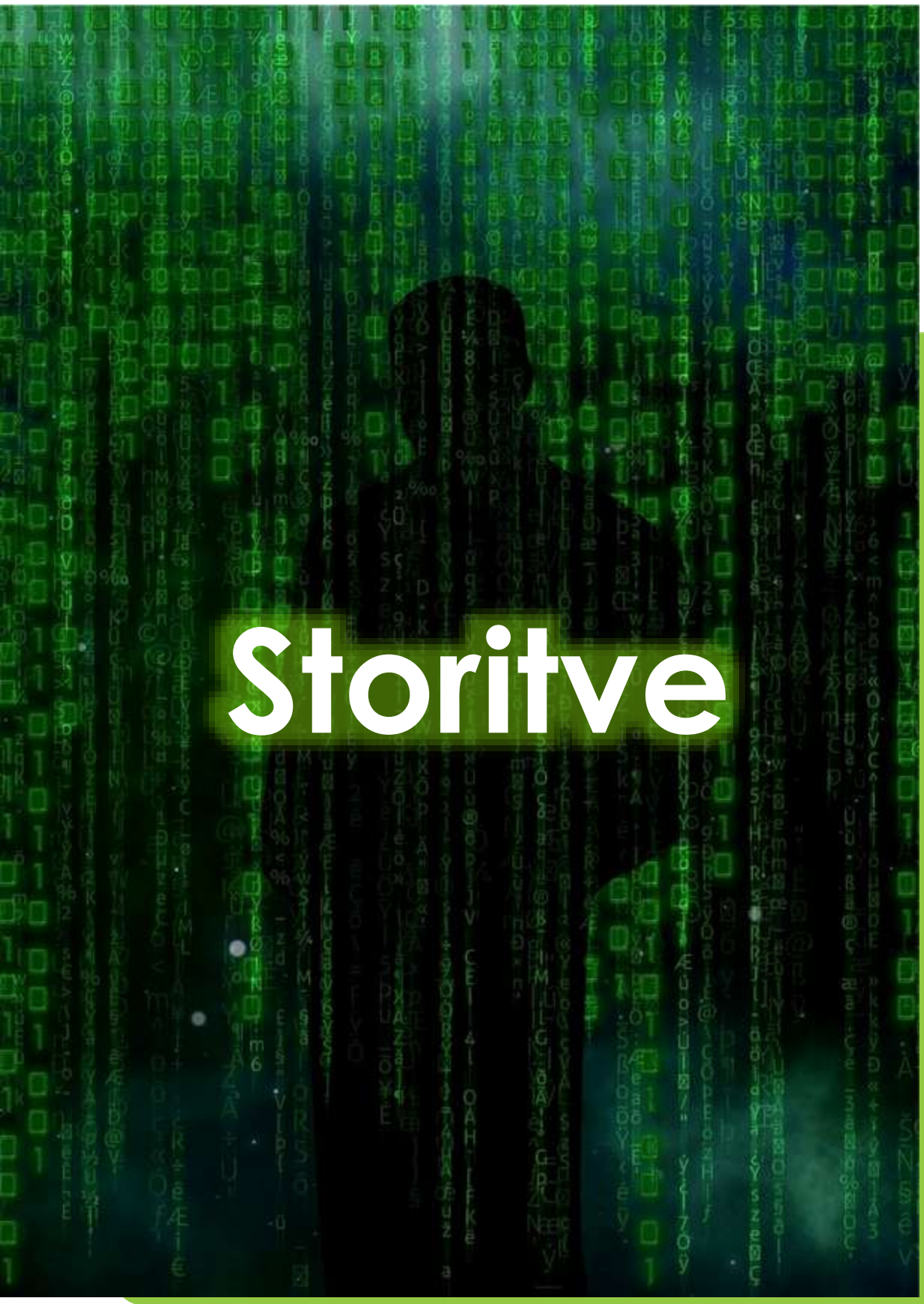
Bistveni subjekti → nad €50 mio letnega prometa; več kot 250 zaposlenih.

Pomembni subjekti → nad €10 mio letnega prometa; več kot 50 zaposlenih.

Dodatno se podjetja delijo na visoko kritične in druge kritične sektorje, kjer pa se velikosti podjetja ne upošteva.

Sektroji kritične in pomembne infrastrukture





Storitev varnostno operativnega centra VOC (ang. SOC)

Varnostno operativni center (VOC) je ključna enota za spremljanje, zaznavanje, preprečevanje in odzivanje na kibernetske grožnje znotraj državnih organov, kritične infrastrukture in poslovnega sektorja, vključno z bančnim sistemom, zavarovalnicami in večjimi podjetji.

Glavne dejavnosti VOC vključujejo:

- Spremljanje in zaznavanje groženj
- Odzivanje na incidente
- Preprečevanje prihodnjih napadov
- Analiza in poročanje
- Povezovanje z drugimi varnostnimi organizacijami

Pomen VOC za državne organe, kritično infrastrukturo in poslovni sektor

Implementacija in delovanje VOC znotraj državnih organov, sektorjev kritične infrastrukture, finančnega sistema in poslovnega sektorja prinaša številne prednosti:

- **Izboljšana zaščita**: VOC zagotavlja boljšo zaščito pred kibernetskimi napadi, kar je ključno za ohranjanje delovanja kritične infrastrukture, finančnih sistemov in podjetij ter zaščito nacionalne varnosti.
- **Hitrejši odziv na incidente**: VOC omogoča hiter in usklajen odziv na varnostne incidente, kar zmanjšuje škodo in pospešuje obnovo sistemov.
- **Preprečevanje napadov**: VOC aktivno deluje na preprečevanju prihodnjih napadov z uvajanjem naprednih varnostnih ukrepov in ozaveščanjem zaposlenih.
- **Povečana zanesljivost in zaupanje**: VOC prispeva k zanesljivosti sistemov in storitev, kar povečuje zaupanje državljanov, strank, investitorjev in partnerjev.
- **Prilagodljivost na nove grožnje**: VOC je sposoben hitro prilagoditi varnostne ukrepe glede na nove in nastajajoče grožnje, kar zagotavlja stalno zaščito in izboljšave varnostnega stanja.

Virtualni CISO (Chief Information Security Officer)

Vitualni CISO (vCISO) je storitev, ki podjetjem omogoča dostop do stokovnjaka za informacijsko varnost brez potrebe po stalni zaposlitvi. Virtualni CISO deluje kot svetovalec na zahtevo in nudi strateško vodstvo na področju varnosti informacij. Ključna prednost je fleksibilnost, saj se storitev prilagaja specifičnim potrebam podjetja in zagotavlja strokovno podporo po meri, ne glede na velikost podjetja ali panogo.

Naloge vCISO-ja

Virtualni CISO opravlja enake naloge kot interno zaposlen CISO. Te vključujejo:

- Razvoj in implementacija varnostnih politik
- Ocena tveganj
- Odziv na incidente
- Izobraževanje in ozaveščanje
- Pomoč pri skladnosti z zakonodajo

Prednosti vCISO storitve

- **Stroškovna učinkovitost:** Namesto visokih stroškov za zaposlitev stalnega CISO, podjetja plačujejo le za storitve, ki jih dejansko potrebujejo.
- **Dostop do vrhunskih strokovnjakov:** Virtualni CISO-ji so izkušeni strokovnjaki z bogatimi izkušnjami na področju varnosti informacij, ki so pridobljene v različnih panogah.
- **Fleksibilnost:** vCISO lahko deluje na daljavo ali v kombinaciji z obiski na lokaciji, kar omogoča prilagoditev storitev specifičnim potrebam podjetja.
- **Hitra odzivnost:** Ker so kibernetske grožnje vedno prisotne, vCISO zagotavlja hitro ukrepanje v primeru incidentov in svetovanje v realnem času.

Storitev virtualnega CISO je idealna rešitev za podjetja, ki želijo učinkovito upravljati kibernetsko varnost brez potrebe po stalni zaposlitvi dragega strokovnjaka. Z vCISO-jem podjetja dobijo dostop do znanja in izkušenj na najvišji ravni ter lahko izboljšajo svojo varnostno držo, zmanjšajo tveganja in izpolnijo zahteve zakonodaje. Ta pristop omogoča strateško in stroškovno učinkovito varovanje podjetniških virov in podatkov.

Penetracijsko testiranje (Pen Test)

Penetracijsko testiranje je simuliran kibernetski napad na informacijski sistem, ki ga izvajajo strokovnjaki za kibernetsko varnost, imenovani etični hekerji. Cilj tega testiranja je odkriti ranljivosti, pomanjkljivosti in šibke točke, ki bi jih hekerji lahko uporabili za dostop do občutljivih podatkov ali povzročitev motenj v delovanju sistema.

Testiranje poteka na več ravneh – od preverjanja omrežij in aplikacij do testiranja fizičnih varnostnih ukrepov. Rezultati so podrobno analizirani, podjetje pa prejme priporočila za izboljšanje varnosti, ki so zasnovana na najdenih ranljivostih.

Prednosti penetracijskega testiranja

- **Zgodnje odkrivanje ranljivosti:** Pent test omogoča odkrivanje in odpravljanje varnostnih lukenj, preden jih lahko izkoristijo napadalci.
- **Povečanje ozaveščenosti o varnosti:** S testiranjem organizacija pridobi vpogled v svoje šibke točke in izboljša ozaveščenost zaposlenih glede kibernetskih groženj.
- **Skladnost z regulativami:** Mnoga podjetja morajo izvajati penetracijska testiranja zaradi skladnosti z zakonodajnimi zahtevami, kot so GDPR, NIS 2, ISO 27001.
- **Preprečevanje finančne škode**: S proaktivnim pristopom k varnosti podjetja zmanjšujejo tveganje finančnih izgub, ki so lahko posledica uspešnega kibernetskega napada ali vdora.

VRSTE PEN TESTIRANJ

Zunanji pent test:

Ta tip testiranja vključuje simulacijo napada na zunanje mreže in aplikacije, ki so dostopne preko interneta. Namenjen je preverjanju, kako dobro so zaščiteni javni deli informacijskega sistema podjetja.

Notranji pent test:

Simulira napad iz notranjosti organizacije, kar je pomembno za preverjanje, kako dobro so varovani sistemi pred napadi, ki bi jih izvedli zaposleni ali drugi interni uporabniki.

Aplikacijski pent test:

Osredotočen je na varnost specifičnih aplikacij, zlasti spletnih in mobilnih aplikacij, ki lahko vsebujejo ranljivosti, kot so vektorski napad SQL, skriptiranje med mesti (XSS) ali pomanjkljivo avtentikacijo.

Socialni inženiring:

Ta tip testiranja preverja pripravljenost zaposlenih na kibernetske napade s tehniko zavajanja (npr. phishing e-pošta), ki izkorišča človeški faktor za pridobivanje dostopa do sistemov.

Proces izvajanja Pen testa

1. **Načrtovanje in obseg:**

Določi se cilje testiranja, področje delovanja in metode, ki jih bodo etični hekerji uporabili.

2. **Zbiranje informacij:**

Testirna ekipa zbira podatke o tarčnem sistemu, kot so naslovi IP, odprta vrata, storitve in ranljivosti.

3. **Izvedba napada:**

Strokovnjaki simulirajo različne napade, pri čemer uporabljajo tehnike, ki jih hekerji uporabljajo v resničnih napadih.

4. **Analiza rezultatov in poročanje:**

Po končanem testu sledi priprava poročila, ki vsebuje vse odkrite ranljivosti in priporočila za izboljšave.

5. **Odprava ranljivosti:**

Podjetje prejme navodila, kako odpraviti odkrite ranljivosti in okrepiti svojo varnostno držo.

Penetracijsko testiranje je ena izmed ključnih komponent proaktivnega pristopa k informacijski varnosti.

S simulacijo kibernetskih napadov lahko podjetja izboljšajo svoje varnostne ukrepe, zmanjšajo tveganje napadov in zavarujejo svoje občutljive podatke. Pent test omogoča, da podjetje odkrije svoje šibke točke in jih odpravi, preden jih lahko zlorabijo hekerji.

Pregled dobavne verige glede trenutnega stanja kibernetske varnosti

Pregled kibernetske varnosti v dobavni verigi je postopek ocenjevanja varnostnih tveganj in zmogljivosti vseh dobaviteljev in partnerjev, ki sodelujejo z organizacijo.

Cilj tega pregleda je identificirati šibke točke, ki bi lahko predstavljale grožnjo za varnost podatkov, ter zagotoviti skladnost z varnostnimi standardi, kot so NIS2, ISO 27001 in drugi relevantni predpisi.

Ključni elementi pregleda dobavne verige

- Ocena tveganj dobaviteljev: Vsak dobavitelj ali partner v dobavni verigi predstavlja določeno stopnjo tveganja. Pregled oceni, kako varnostni sistemi in prakse dobaviteljev vplivajo na varnost celotne verige.
- Skladnost z varnostnimi standardi: Pregled zagotavlja, da vsi dobavitelji izpolnjujejo ključne varnostne zahteve, predpisane z zakonodajo in industrijskimi standardi, kot so zaščita podatkov, nadzor dostopa, incidentno odzivanje in drugi.
- Testiranje varnostnih politik in praks: V okviru pregleda se preverja, ali dobavitelji izvajajo ustrezne varnostne ukrepe, kot so šifriranje podatkov, nadzor dostopa, usposabljanje zaposlenih in redno posodabljanje varnostnih sistemov.
- Ocenjevanje upravljanja incidentov: Dobri dobavitelji imajo vzpostavljene politike za odzivanje na kibernetske incidente in so sposobni hitro ukrepati v primeru napada, kar zmanjšuje morebitno škodo.
- Kibernetska odpornost dobavne verige: Pregled se osredotoča tudi na dolgoročno odpornost dobavne verige, kar vključuje sposobnost dobaviteljev, da se prilagodijo novim grožnjam in izvajajo potrebne varnostne izboljšave.

Kako poteka pregled?

1. Identifikacija ključnih dobaviteljev: Najprej se določi, kateri dobavitelji so ključni za delovanje podjetja in dostopajo do občutljivih podatkov.
2. Ocena varnostnih ukrepov dobaviteljev: Analizirajo se varnostni postopki, politike in tehnologije, ki jih dobavitelji uporabljajo za zaščito podatkov in sistemov.
3. Identifikacija tveganj: Na podlagi zbranih podatkov se oceni stopnja tveganja, ki ga predstavlja vsak dobavitelj, ter določi morebitne pomanjkljivosti.
4. Izdelava poročila in priporočil: Po pregledu se pripravi poročilo s podrobno analizo ugotovitev in predlogi za izboljšanje varnosti v celotni dobavni verigi.

Kibernetska varnost dobavne verige je ključnega pomena za zaščito podjetij pred vedno večjimi grožnjami. S pregledom kibernetske varnosti v dobavni verigi lahko podjetja učinkovito ocenijo tveganja, ki jih prinašajo njihovi dobavitelji, in s tem zagotovijo celovito zaščito svojih informacijskih sistemov in podatkov. To prispeva k dolgoročni odpornosti, skladnosti z zakonodajo in večji zaupljivosti v partnerstvih.

Prednosti pregleda

- Prepoznavanje ranljivosti: Sistematičen pregled omogoča prepoznavanje šibkih točk v dobavni verigi, ki bi lahko bile tarča kibernetskih napadov.
- Zmanjšanje tveganja napadov: Z ocenjevanjem in nadzorom nad varnostjo dobaviteljev lahko podjetje zmanjša verjetnost napada, ki bi izviral iz slabše zavarovanih povezav v verigi.
- Skladnost z zakonodajo: Pregled zagotavlja, da podjetje in vsi njegovi dobavitelji izpolnjujejo ustrezne regulativne zahteve in standarde glede varovanja podatkov.
- Krepitev zaupanja med partnerji: Reden pregled varnosti v dobavni verigi povečuje zaupanje med podjetjem in njegovimi partnerji ter izboljšuje sodelovanje.

Pregled “deep web intelligence”

Pregled deep in dark weba je storitev pregleda spleta, ki uporablja napredne tehnologije za iskanje, spremljanje in analizo podatkov iz neindeksiranih in težje dostopnih delov interneta, kot so temni forumi, zasebni trgi in klepetalnice, kjer hekerji pogosto izmenjujejo informacije o ranljivostih, ukradenih podatkih, napadih in zlonamerni programski opremi. Cilj te storitve je zagotoviti vpogled v potencialne nevarnosti, ki bi lahko vplivale na podjetje.

Kako deluje pregled temnega spleta?

Poslužuje se uporabe specializiranih orodij in tehnik za spremljanje aktivnosti na dark webu, deep webu in drugih neindeksiranih virih. Strokovnjaki za kibernetsko varnost spremljajo ključne teme, ki bi lahko bile povezane s podjetjem ali industrijo, kot so:

- Prodaja ukradenih podatkov: Zaznavajo se primeri, ko se občutljivi podatki, kot so gesla, osebni podatki ali podatki o kreditnih karticah, pojavljajo na črnih trgih.
- Razprava o ranljivostih: Identificirajo se ranljivosti, ki jih hekerji razpravljajo ali načrtujejo izkoristiti.
- Načrtovani kibernetski napadi: Odkrijejo se znaki pripravljanja napadov, kot so phishing kampanje, napadi z odkupno programsko opremo ali druge vrste zlonamernih aktivnosti.

Kako poteka pregled temnega spleta?

1. Spremljanje in zaznavanje: Strokovnjaki za kibernetsko varnost uporabljajo specializirana orodja za spremljanje deep weba, dark weba in drugih virov, kjer se pojavljajo kibernetske grožnje.
2. Analiza groženj: Pridobljeni podatki se analizirajo, da se določi resnost groženj in kako bi lahko vplivali na podjetje.
3. Poročanje in priporočila: Podjetje prejme redna poročila o zaznanih grožnjah, skupaj s priporočili za ukrepanje, da bi zmanjšali tveganje za napade.

Pregled temnega spleta predstavlja ključni del sodobne kibernetske obrambe. S to storitvijo podjetja pridobijo vpogled v temne kotičke interneta, kjer lahko pravočasno zaznajo grožnje in ukrepajo še preden te dosežejo njihovo okolje. To omogoča boljšo pripravljenost na prihodnje kibernetske izzive in učinkovito zaščito pred napadi.

Breach and Attack Simulation (BAS)

Breach and Attack Simulation je storitev, ki omogoča simulacijo različnih kibernetskih napadov in vdorov v realnem času, s čimer podjetja testirajo svoje varnostne sisteme in postopke. Cilj BAS je preizkusiti, kako učinkovito se varnostna infrastruktura podjetja odziva na napade, kot so vdori, okužbe z zlonamerno programsko opremo, kraje podatkov in drugi incidenti. BAS simulira resnične napade brez povzročanja dejanske škode, kar omogoča prepoznavanje ranljivosti v varnostnih sistemih.

Kako deluje BAS?

BAS platforma avtomatizira izvajanje različnih vrst napadov, ki temeljijo na znanih taktikah, tehnikah in postopkih (TTP), ki jih uporabljajo napadalci. Storitev vključuje:

- Simulacijo kibernetskih napadov: Varnostni strokovnjaki uporabljajo napredna orodja za simulacijo različnih vrst napadov, kot so phishing napadi, DDoS napadi, eksfiltracija podatkov in druge zlonamerne dejavnosti.
- Preizkus varnostnih kontrol: BAS preizkusi, kako učinkovito delujejo obstoječe varnostne kontrole, kot so požarni zidovi, protivirusna programska oprema, sistemi za odkrivanje in preprečevanje vdora (IDS/IPS) ter odzivne zmogljivosti.
- Neprekinjeno testiranje: Simulacije potekajo v realnem času in neprekinjeno, kar podjetjem omogoča stalno spremljanje varnostnega stanja ter hitro ukrepanje ob odkritih ranljivostih.

Skladnost s standardi

Simulacije lahko pomagajo pri doseganju skladnosti z varnostnimi standardi in regulativnimi zahtevami, kot so NIS2, ISO 27001 in drugi, saj zagotavljajo jasen vpogled v varnostno stanje organizacije.

Ključni elementi Breach and Attack Simulation

1. Prepoznavanje ranljivosti: BAS omogoča prepoznavanje šibkih točk v omrežju, aplikacijah ali procesih, ki bi jih lahko napadalci izkoristili za dostop do občutljivih podatkov ali onemogočanje sistemov.
2. Testiranje varnostne pripravljenosti: Simulacije testirajo pripravljenost podjetja na različne vrste napadov, vključno z notranjimi grožnjami, zunanjimi napadi in napadi ciljnih hekerskih skupin.
3. Neprekinjeno izboljševanje varnostne strategije: BAS ne zagotavlja le enkratnega pregleda, ampak podjetjem omogoča stalno preverjanje varnostnih kontrol in izboljševanje varnostne strategije na podlagi novih podatkov o grožnjah.
4. Ocenjevanje odzivnih ukrepov: Simulacije pomagajo preizkusiti, kako hitro in učinkovito se podjetje odzove na kibernetski incident, kar vključuje tako tehnične kot organizacijske ukrepe.

Kako poteka Breach and Attack Simulation?

1. Načrtovanje simulacij: Na podlagi potreb podjetja in specifičnih varnostnih tveganj se oblikujejo scenariji simuliranih napadov.
2. Izvedba simulacij: BAS platforma simulira različne kibernetske napade v nadzorovanem okolju, brez dejanskih motenj v poslovanju.
3. Analiza rezultatov: Po zaključku simulacij se pridobijo podrobni podatki o učinkovitosti varnostnih kontrol, zaznanih ranljivostih in odzivnih ukrepih.
4. Poročanje in priporočila: Podjetje prejme poročilo z ugotovitvami in priporočili za izboljšanje varnostnih ukrepov, kar vključuje izboljšave v omrežni varnosti, vzpostavitev boljših zaščitnih ukrepov in okrepitev odzivnih postopkov.

Breach and Attack Simulation predstavlja sodobno, napredno rešitev za zagotavljanje visoke stopnje kibernetske varnosti. S simulacijo resničnih napadov BAS podjetjem omogoča prepoznavanje ranljivosti, izboljšanje varnostnih politik in postopkov ter krepitev celovite pripravljenosti na kibernetske grožnje. To je ključno za zagotavljanje stalne varnosti in zaščito pred napadi, ki bi lahko imeli resne posledice za poslovanje.

Red Teaming

Red Teaming je simulacija ciljnih napadov, ki jih izvajajo visoko usposobljeni strokovnjaki (rdeča ekipa) v nadzorovanem okolju, da preizkusijo sposobnost organizacije za odkrivanje in odzivanje na napade. Cilj te simulacije ni zgolj najti tehnične pomanjkljivosti v varnostnih sistemih, temveč preveriti tudi pripravljenost podjetja na strateški in operativni ravni. Red Teaming vključuje napredne tehnike, ki jih uporabljajo hekerji, vključno s socialnim inženiringom, fizičnimi vdori in tehničnimi napadi.

Kako deluje Red Teaming?

Red Teaming je večstopenjski proces, ki vključuje:

- Načrtovanje in raziskovanje: Rdeča ekipa najprej raziskuje podjetje in analizira njegove ranljivosti, da določi najbolj učinkovite metode za napad. Ta faza vključuje zbiranje informacij o zaposlenih, omrežju, infrastrukturi in sistemih.
- Izvajanje napadov: Rdeča ekipa nato simulira ciljne napade, ki temeljijo na tehnikah, kot so socialni inženiring, phishing kampanje, zloraba ranljivosti, fizični vdori in napadi na omrežje.
- Izogibanje zaznavi: Rdeča ekipa poskuša napade izvajati tako, da jih varnostni sistemi podjetja ne zaznajo, kar omogoča preizkus resnične sposobnosti za odkrivanje kibernetskih groženj.

Ključni elementi Red Teaming storitev

1. Simulacija realnih napadov: Red Teaming posnema resnične kibernetske napade, pri čemer strokovnjaki delujejo kot nasprotnik, ki poskuša zaobiti vse varnostne ovire podjetja.
2. Socialni inženiring: Napadi vključujejo tehnike, kot so phishing in manipulacija zaposlenih, kar je ključni del strategije napadalcev.
3. Napadi na omrežje in sisteme: Rdeča ekipa izvaja napade na tehnične sisteme in omrežje, da ugotovi, kako dobro so zaščiteni pred notranjimi in zunanjimi napadi.
4. Testiranje odziva modre ekipe (Blue Team): Red Teaming pogosto poteka skupaj z Blue Team (obrambno) ekipo, kar omogoča oceno, kako učinkovito podjetje zazna in se odzove na napade v realnem času.

Prednosti Red Teaming-a

- **Realističen vpogled v varnostni sistem:** Red Teaming omogoča vpogled v dejansko stanje kibernetske varnosti podjetja, saj simulira najnaprednejše napade.
- **Zmanjšanje tveganja:** Z odkrivanjem skritih ranljivosti in pomanjkljivosti lahko podjetja pred napadi izboljšajo svoje varnostne politike in postopke.
- **Preizkus odzivnosti podjetja**: Storitev pomaga oceniti, kako učinkovito se podjetje odziva na kibernetske grožnje, ter identificirati morebitne šibkosti v odzivnih postopkih.
- **Izboljšanje varnostne strukture**: Z uporabo socialnega inženiringa in drugih tehnik rdeče ekipe se lahko izboljša ozaveščenost zaposlenih o grožnjah in ranljivostih, ki jih lahko hekerji izkoristijo.

Kako poteka Red Teaming?

1. Faza načrtovanja: Na začetku Red Teaming operacije se določijo specifični cilji, metode in obseg testiranja. Rdeča ekipa zbere potrebne informacije o podjetju in izbere najbolj verjetne poti napada.
2. Izvedba napadov**:** Rdeča ekipa izvede ciljno usmerjene napade na podjetje oziroma subjekt, pri čemer skuša neopaženo prodreti v sisteme. Simulacija vključuje celoten spekter možnih napadov, od tehničnih do fizičnih.
3. Analiza in poročanje: Po končanih napadih rdeča ekipa pripravi obsežno poročilo o najdenih ranljivostih in uspešnosti napadov. Poročilo vključuje tudi priporočila za izboljšave.
4. Izvedba izboljšav: Na podlagi ugotovitev lahko podjetje hitro odpravi zaznane ranljivosti, izboljša svoje varnostne politike in okrepi pripravljenost na prihodnje napade.

Z realističnimi simulacijami napadov podjetja pridobijo vpogled v svoje varnostne vrzeli in izboljšajo sposobnost odkrivanja ter odzivanja na grožnje. Ta storitev je ključnega pomena za podjetja, ki želijo preizkusiti in okrepiti svojo obrambo pred najnaprednejšimi kibernetskimi grožnjami, ter zmanjšati tveganja za resnične napade.

Analiza skladnosti z NIS 2 (NIS 2 Gap Analysis)

Analiza skladnosti z NIS 2 (Gap Analysis) je celovit postopek pregleda in primerjave trenutnih varnostnih ukrepov podjetja z zahtevami NIS 2 direktive. Namen te storitve je identificirati razkorake (“vrzeli”) med trenutnim stanjem kibernetske varnosti podjetja in zahtevami, ki jih določa direktiva, ter pripraviti načrt za odpravo teh vrzeli. Analiza omogoča podjetjem, da se osredotočijo na kritična področja, ki jih je treba izboljšati, da bi dosegli skladnost z NIS 2 direktivo.

Kako poteka analiza skladnosti z NIS 2?

Ta vključuje več ključnih korakov:

1. Pregled obstoječih varnostnih ukrepov: Analiziramo trenutne kibernetske varnostne politike, postopke, tehnologije in sisteme v podjetju ter ugotavljamo, kako učinkovito ščitijo pred grožnjami in napadi.
2. Primerjava z NIS 2 zahtevami: Podrobno primerjamo obstoječe ukrepe z zahtevami, ki jih določa NIS 2 direktiva. To vključuje preverjanje skladnosti na področjih, kot so upravljanje tveganj, zaščita podatkov, zaznavanje incidentov, odziv na kibernetske napade ter upravljanje varnostnih operacij.
3. Identifikacija vrzeli oziroma pomanjkljivosti: Na podlagi analize identificiramo področja, kjer obstoječi varnostni ukrepi podjetja ne ustrezajo standardom NIS 2. Te vrzeli so lahko povezane s tehničnimi rešitvami, pomanjkanjem ustreznih politik ali neustrezno ozaveščenostjo zaposlenih o varnostnih tveganjih.
4. Priprava načrta za odpravo pomanjkljivosti: Na podlagi ugotovljenih pomanjkljivosti pripravimo podroben načrt za izboljšanje varnostne infrastrukture, postopkov in politik, da bi podjetje doseglo popolno skladnost z NIS 2. Načrt vključuje tudi predloge za izboljšanje zaznavanja in odzivanja na incidente ter krepitev upravljanja varnostnih tveganj.

Zakaj je analiza skladnosti z NIS 2 pomembna?

- **Izpolnjevanje zakonskih obveznosti**: Podjetja, ki spadajo pod področje uporabe NIS 2 direktive, so zakonsko zavezana k zagotavljanju ustrezne kibernetske varnosti. Analiza pomaga ugotoviti, katera področja je treba izboljšati, da bi dosegli skladnost in se izognili kaznim ali pravnim posledicam.

- **Zmanjšanje tveganja za kibernetske napade**: S prepoznavanjem varnostnih vrzeli lahko podjetja izboljšajo svojo obrambo pred kibernetskimi napadi, zmanjšajo tveganje za uspešen napad in zaščitijo kritične podatke ter sisteme.
- **Izboljšanje pripravljenosti na incidente**: Analiza pomaga prepoznati pomanjkljivosti v postopkih odzivanja na incidente, kar omogoča podjetjem, da hitreje in učinkoviteje zaznajo ter obvladajo morebitne kibernetske grožnje.
- **Optimizacija virov**: Z natančno analizo podjetja lažje določijo, kje so potrebne izboljšave, kar omogoča bolj ciljno usmerjeno vlaganje virov v kibernetsko varnost.

Ključni elementi analize skladnosti z NIS 2 direktivo

1. **Pregled upravljanja varnostnih tveganj**: Analiza osredotočena na sisteme, ki podjetju omogočajo spremljanje, zaznavanje in obvladovanje kibernetskih tveganj.
2. **Preizkus skladnosti z zakonodajnimi zahtevami**: Ugotavljanje skladnosti obstoječih varnostnih ukrepov z NIS 2 direktivo, ki zahteva vzpostavitev robustnih varnostnih praks.
3. **Prepoznavanje prioritet**: Na podlagi analize določimo, katera področja zahtevajo takojšnjo pozornost in izboljšave, da bi zmanjšali tveganja.
4. **Priprava poročila**: Končno poročilo vsebuje podrobne ugotovitve o varnostnih vrzelih in priporočila za potrebne ukrepe, da bi podjetje doseglo skladnost z direktivo.

Analiza skladnosti z NIS 2 je ključna storitev za podjetja, ki želijo izpolniti zahteve NIS 2 direktive in izboljšati svojo kibernetsko odpornost. S pomočjo te analize podjetja pridobijo jasen vpogled v svoje varnostne pomankljivosti ter izpolnjene pogoje in prejmejo konkretne usmeritve za izboljšave, kar omogoča doseganje skladnosti ter boljšo zaščito pred vedno večjimi kibernetskimi grožnjami.

Zaključek

Kibernetska varnost je ključna za zaščito občutljivih podatkov, zagotavljanje nemotenega delovanja sistemov in preprečevanje kibernetskih napadov, ki lahko povzročijo resne motnje ali škodo.

Zaradi vse večje digitalizacije in povezljivosti sistemov, kibernetska varnost postaja vedno bolj pomembna saj vpliva na delovanje vseh sektorjev kritične infrastrukture, državnih organov in poslovnega sektorja (vključno z bančnim sistemom, zavarovalnicami in velikimi podjetji).

Z nenehno rastočimi in razvijajočimi se grožnjami morajo podjetja in organizacije sprejeti celovite in napredne storitve in varnostne rešitve, ki omogočajo proaktivno in avtomatizirano zaščito njihovih informacijskih sistemov.

Kibernetska varnost je danes bolj kot kdaj koli prej ključnega pomena za vsako organizacijo in tukaj nastopimo mi, ki pomagamo z našo profesionalno, strokovno ter izkušeno ekipo nuditi našim strankam inovativne in najkvalitetnejše storitve ter rešitve za kibernetsko varnost, s čimer se lahko organizacije in podjetja zaradi tega osredotočijo na svoj glavni pomen.

THZ NETWORKS – Oddelek za kibernetsko varnost

https://www.thz.net/

Certifikati naših strokovnjakov