Od Modre, Vijolične in Rdeče do Črne

Matej Perhavec

Sportradar d.o.o., Ljubljana, Slovenija
m.perhavec@sportradar.com

V sodobnem digitalnem okolju organizacije letno namenjajo velik del svojih sredstev za krepitev kibernetsko-varnostnih zmogljivosti, predvsem z namenom zaščite pred oddaljenimi, pogosto anonimnimi napadalci. Ob tem se zastavlja pomembno vprašanje: koliko pozornosti je pri tem namenjeno fizični varnosti? Ali obstoječe organizacijske skupine znotraj kibernetske varnosti, kot so modra, rdeča in vijolična ekipa, res zadoščajo za učinkovito obvladovanje varnostnih tveganj ali pa vse večja izpostavljenost fizičnim grožnjam narekuje potrebo po dodatni, specializirani skupini? V prispevku smo predstavili že uveljavljene varnostne ekipe na področju kibernetske varnosti (modro, rdečo in vijolično), osredotočili pa smo se na še ne tako prepoznavno a vseeno ključno črno ekipo, katere osrednja naloga je izvajanje fizičnih penetracijskih testov in varnostnih pregledov. Opisali smo njene glavne aktivnosti in metodologijo, umestili njeno vlogo v kontekstu nove evropske direktive CER in poudarili sodelovanje črne ekipe z drugimi varnostnimi skupinami. Predstavili smo tudi konkretne primere fizičnih ranljivosti z digitalno komponento, ki dodatno potrjujejo pomen vključevanja črne ekipe v kibernetsko-varnostno strategijo organizacij.

Ključne besede:
modra ekipa,
rdeča ekipa,
vijolična ekipa,
črna ekipa,
fizično penetracijsko testiranje,
fizični varnostni pregledi,
fizična varnost.

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-299-037-4
DOI https://doi.org/10.18690/um.feri.7.2025.13

1 Uvod

V sodobni kibernetski varnosti se za opis ključnih vlog in pristopov pogosto uporablja barvna klasifikacija namenskih skupin, kot so modra ekipa (angl. blue team), rdeča ekipa (angl. red team), vijolična ekipa (angl. purple team) in črna ekipa (angl. black team), ki označujejo specializirane organizacijske enote z različnimi odgovornostmi za zaščito in testiranje informacijskih sistemov.

Izraza Blue Team in Red Team izvirata iz vojaške prakse, kjer so skupine za simulacijo bojev zasedale vloge branilcev in napadalcev, da bi izboljšale taktiko, pripravljenost in odzivnost na sovražne sile. Tradicionalno je bila rdeča barva simbol nasprotnikov oziroma napadalcev, medtem ko je modra barva predstavljala zavezniške oziroma obrambne enote. Ta simbolika se je kasneje prenesla v informacijsko varnost, kjer rdeča ekipa prevzema vlogo simuliranih napadalcev, medtem ko modra ekipa deluje kot obrambna enota, ki zaznava in preprečuje grožnje [1].

Z naraščajočo kompleksnostjo kibernetskih napadov in potrebo po bolj učinkovitem sodelovanju med napadalskimi in obrambnimi ekipami se je uveljavil koncept vijolične ekipe. Vijolična ekipa združuje znanja in veščine rdeče in modre ekipe v sodelovanje, ki omogoča hitrejše odkrivanje varnostnih pomanjkljivosti in neposredno izboljšanje varnostnih ukrepov. Ta pristop se je uveljavil kot odgovor na potrebe po agilnosti in stalnem prilagajanju varnostnih sistemov glede na nove tehnike napadalcev.

Črna ekipa, ki se osredotoča na fizično penetracijsko testiranje in fizično varnost organizacij, izvira iz varnostnih in vojaških praks testiranja fizičnih varnostnih ukrepov, kot so kontrole dostopa, varnostno osebje in postopki za zaščito kritične infrastrukture. S prihodom digitalizacije in integracije fizičnih in kibernetskih varnostnih elementov se je pomen črne ekipe okrepil kot ključni del celostne varnostne strategije. Pristopi črne ekipe so danes nepogrešljivi pri prepoznavanju ranljivosti, ki izhajajo iz fizičnega dostopa do sistemov, kar pogosto predstavlja začetek kibernetskih incidentov.

Ti štirje koncepti skupaj tvorijo celosten okvir za varnostne prakse, ki vključujejo simulacijo napadov, obrambno odzivnost, sodelovanje ekip in fizično varnost, s ciljem povečanja odpornosti organizacij na sodobne varnostne grožnje.

2 Modra ekipa

Modra ekipa predstavlja osrednji obrambni mehanizem organizacije, katerega ključna naloga je zagotavljanje celovite zaščite informacijskih sistemov, omrežij in podatkov pred različnimi vrstami kibernetskih groženj. Njeno delovanje temelji na stalnem spremljanju varnostnih dogodkov, zaznavanju anomalij, analizi groženj ter izvajanju tehničnih in organizacijskih ukrepov za preprečevanje, odkrivanje in odzivanje na varnostne incidente.

Ključno operativno okolje za delovanje modre ekipe predstavlja VOC[2] (angl. SOC[3]), ki je zadolžen za zbiranje in analizo dnevniških zapisov, opozoril in dogodkov iz različnih virov, vključno z IDS[4]/IPS[5] sistemi, požarnimi zidovi, SIEM[6] in EDR[7]/XDR[8] rešitvami. VOC tako omogoča modri ekipi pravočasen vpogled v stanje varnosti informacijskega okolja in koordiniran odziv na zaznane grožnje.

[2] VOC - Varnostni Operativni Center
[3] SOC - Security Operations Center
[4] IDS - Intrusion Detection System
[5] IPS - Intrusion Prevention System
[6] SIEM - Security Information and Event Management
[7] EDR - Endpoint Detection and Response
[8] XDR - Extended Detection and Response

Pomemben del funkcionalnosti modre ekipe predstavlja tudi odziv na incidente (angl. incident response), ki je natančno opredeljen v okviru smernic NIST SP 800-61r3 [2] in vključuje štiri faze:

- pripravo,
- zaznavo in analizo,
- zajezitev, odpravo in obnovitev,
- zaključne aktivnosti z analizo po incidentu.

Strukturiran odziv na incidente skrajša čas zaznave in odprave (MTTD[9]/MTTR[10]) ter posledično prispeva k zmanjšanju vpliva varnostnih dogodkov.

Modra ekipa prav tako izvaja lov na grožnje (angl. threat hunting), ki predstavlja proaktiven in hipotezno usmerjen (angl. hypothesis-driven) proces iskanja naprednih, pogosto prikritih groženj znotraj informacijskega okolja organizacije. Ta proces temelji na analizah vedenjskih vzorcev, zgodovinskih podatkov in groženj iz zunanjih virov (npr. uporaba MITRE ATT&CK ogrodja) [3]. Lov na grožnje presega pasivne obrambne ukrepe; omogoča identifikacijo napadalcev, ki so se morda že infiltrirali v sistem, a še niso povzročili zaznanih škodljivih posledic.

Poleg omenjenih osrednjih nalog modra ekipa izvaja tudi upravljanje ranljivosti (angl. vulnerability management), ki obsega redno izvajanje ocen ranljivosti (angl. vulnerability assessments) z uporabo avtomatiziranih orodij kot so skenerji ranljivosti (angl. vulnerability scanner), ter vzpostavitev procesov za odpravo kritičnih pomanjkljivosti s pomočjo vpeljave varnostnih popravkov (angl. patch management). Ti postopki omogočajo zmanjšanje napadalne površine ter preprečevanje izkoriščanja znanih ranljivosti. Modra ekipa aktivno sodeluje tudi pri načrtovanju odziva na incidente in vpeljevanju kriznih načrtov.

Kot ključni obrambni člen v celostnem okviru kibernetske varnosti modra ekipa omogoča proaktivno obvladovanje varnostnih dogodkov, zgodnje odkrivanje napadalcev in učinkovito zmanjševanje posledic incidentov. Njeno delovanje neposredno prispeva k stabilnosti poslovanja in zrelosti celotne varnostne strategije organizacije.

3 Rdeča ekipa

Rdeča ekipa predstavlja specializirano varnostno skupino, katere ključne naloge vključujejo penetracijsko testiranje, simulacije napadov, izvajanje socialno-inženirskih kampanj in celovitih red teaming aktivnosti z namenom preverjanja učinkovitosti obrambnih zmogljivosti organizacije.

Penetracijsko testiranje temelji na odkrivanju in izkoriščanju odkritih ranljivosti z namenom preverjanja odpornosti sistemov, aplikacij in omrežij ter se izvaja v skladu s smernicami NIST SP 800-115 [4] in metodologijami, kot so PTES[11], OWASP[12] Testing Guide in OSSTMM[13]. Razlika med penetracijskim testiranjem in red teaming aktivnostmi je v ciljih in pristopu: medtem ko je pri penetracijskem testiranju cilj odkriti čim več ranljivosti, se pri red teaming aktivnostih rdeča ekipa osredotoča na neopažen doseg specifičnih ciljev, kot so kompromitacija domenskega krmilnika, dostop do zaupnih podatkov ali dolgotrajen in prikrit dostop do interne infrastrukture.

Poleg specifičnih ciljev, red teaming aktivnosti celovito in realistično preverjajo odpornost organizacije na napade, pri čemer posnemajo taktike, tehnike in postopke (angl. TTP[14]) dejanskih napadalcev. Zajemajo širok spekter simuliranih napadov, vključno s socialnim inženiringom, fizičnim vdorom in preizkusom operativne varnosti.

[9] MTTD - Mean Time To Detect
[10] MTTR - Mean Time To Repair
[11] PTES - Penetration Testing Execution Standard
[12] OWASP - Open Worldwide Application Security Project
[13] OSSTMM - Open Source Security Testing Methodology Manual
[14] TTP - Tactics, Techniques and Procedures

Takšen pristop omogoča realistično simulacijo napadov naprednih trajnih groženj (angl. APT[15]), katere cilj je ocena dejanske pripravljenosti modre ekipe, zlasti varnostno operativnega centra in njene odzivnosti na incidente.

Posebnost red teaming aktivnosti je vključevanje fizičnih vektorjev napada za doseg zadanih kibernetskih ciljev, kar predstavlja pomembno komponento celostnega testiranja. V skladu z metodologijo OSSTMM Chapter 8 - Physical Security Testing [5] in smernicami ISO/IEC 27001 [6] in 27002 [7] ter NIST SP 800-53r5 [8] o fizični varnosti, se v sklopu red teaming aktivnosti preverja varnost fizičnih dostopov, nadzor in segmentacija dostopov znotraj organizacije in ozaveščenost zaposlenih. Primeri fizičnih testov vključujejo poskuse neopaznega vstopa v stavbo (npr. tailgating), namestitev nepooblaščenih naprav (npr. keylogger), socialni inženiring (npr. uporaba lažne identitete vzdrževalca) ali izkoriščanje slabih fizičnih praks (npr. nezaščiten dostop do strežniške sobe).

Rdeča ekipa z realističnim, nadzorovanim in etičnim testiranjem tako ne le razkriva tehnične pomanjkljivosti, temveč preverja tudi odpornost na človeške napake, socialni inženiring in fizično varnost. Njihovo delovanje predstavlja eno najpomembnejših orodij za organizacije, ki si prizadevajo doseči visoko stopnjo varnostne zrelosti in operativne pripravljenosti.

4 Vijolična ekipa

Vijolična ekipa predstavlja metodološki in organizacijski pristop k izboljšanju kibernetske varnosti z aktivnim povezovanjem dveh tradicionalno ločenih skupin - rdeče ekipe (simuliranje napadov) in modre ekipe (obramba pred napadi). Namesto ločenega delovanja, skupen pristop omogoča usklajeno sodelovanje med obema ekipama z namenom neposredne izmenjave znanja, testiranja zaznavnih zmožnosti in sprotnega prilagajanja obrambnih mehanizmov glede na dejanske tehnike napadalcev.

Ključna značilnost takšnega sodelovanja je sprotno pridobivanje povratnih informacij: ko rdeča ekipa izvede specifičen napad ali tehniko (npr. lateral movement ali privilege escalation), modra ekipa sočasno spremlja sposobnost zaznave dogodkov ter nato skupaj z rdečo ekipo analizira vrzeli v zaznavi, odzivu ali eskalaciji. Takšen pristop pogosto temelji na vzorcu »assume breach«, ki predpostavlja, da se je napadalcu že uspelo infiltrirati v sistem ali omrežje in preverja, kako globoko lahko napadalec prodre znotraj organizacije. Vse to poteka v varnem in nadzorovanem okolju, s ciljem izboljšati detekcijo, notranjo segmentacijo in odzivnih zmogljivosti.

Pri delu vijolične ekipe se uporabljajo tako ročna kot avtomatizirana ogrodja za simulacije napadov. Med ročnimi ogrodji izstopata ogrodji Atomic Red Team [9] in Caldera [10], ki omogočata izvajanje posameznih taktik, tehnik in postopkov z namenom preverjanja zaznavnih zmožnosti obrambnih orodij. Hkrati se v okviru aktivnosti uporabljajo tudi avtomatizirana orodja za simulacijo vdorov in napadov (npr. BAS[16]), ki omogočajo ponovljivost, standardizacijo ter kontinuirano validacijo učinkovitosti obrambnih mehanizmov.

Vpeljava vijolične ekipe v varnostno arhitekturo omogoča hitrejšo izpopolnjevanje varnostnih mehanizmov, ciljno usmerjeno zaznavanje in boljšo usklajenost med varnostnimi in poslovnimi cilji. Organizacije, ki integrirajo tak pristop v svojo varnostno strategijo, dosegajo višjo stopnjo zrelosti, saj ne odkrivajo zgolj pomanjkljivosti, temveč jih tudi aktivno odpravljajo na način, ki je prilagojen njihovemu okolju.

[15] APT - Advanced Persistent Threat
[16] BAS - Breach and Attack Simulation

5 Črna ekipa

V pogovoru o varnosti in zaščiti organizacij pogosto prevladuje digitalna varnost, vendar fizična varnost ostaja ključen, a pogosto spregledan steber celostne zaščite organizacije. Napadalci ne potrebujejo zmeraj napredne zlonamerne programske opreme ali 0-day ranljivosti, včasih je dovolj fizični dostop do neustrezno zavarovane strežniške sobe ali do sejne sobe kjer vodstven kader sprejema interne odločitve, da nepooblaščene osebe pridejo do ključnih informacij. Tu nastopi črna ekipa - specializirana varnostna enota, katere glavna naloga je preizkušanje in izboljševanje fizične varnosti organizacije.

Črna ekipa se osredotoča na fizično varnost organizacije in njen preplet z digitalno varnostjo. Ključne naloge črne ekipe so fizično penetracijsko testiranje, simulacija vdorov ter socialni inženiring, s čimer organizaciji pomaga odkriti varnostne pomanjkljivosti, povezane s fizičnim dostopom do informacijskih sistemov, kritične infrastrukture in drugih ključnih virov organizacije. Gre za nadzorovane in etične simulacije napadov, ki vključujejo preizkušanje varnostnih sistemov, kot so sistemi kontrole dostopa, alarmni sistemi, kamere, fizične pomanjkljivosti ter ozaveščenost in odzivnost zaposlenih [5].

5.1. Aktivnosti črne ekipe

Delovanje črne ekipe temelji na mednarodno priznanih standardih in smernicah, kot so OSSTMM Chapter 8 - Physical Security Testing [5] in priporočilih Evropske agencije za kibernetsko varnost (ENISA) glede fizične varnosti [11,12]. Poleg izvajanja fizičnih penetracijskih testov in simulacij napadov, črna ekipa zaradi svojega specifičnega nabora znanj in izkušenj s področja fizične in kibernetske varnosti, prav tako izvaja in sodeluje pri izvedbi fizičnih varnostnih in revizijskih pregledov.

Fizično penetracijsko testiranje

Fizično penetracijsko testiranje, je ključnega pomena za odkrivanje ranljivosti, ki jih tehnološki varnostni sistemi ne zaznajo. Primeri simulacij resničnih fizičnih groženj vključujejo: poskuse nepooblaščenega vstopa v stavbe, infiltracijo skozi varnostne preglede, krajo in kloniranje dostopnih kartic, namestitev nepooblaščenih naprav (npr. keylogger, rogue access point) in pridobitev fizičnega dostopa do ključnih organizacijskih prostorov in virov (npr. strežnikov, omrežne opreme, zaupnih dokumentov).

Tako kot pri digitalnem penetracijskem testiranju tudi fizično penetracijsko testiranje poteka po jasno določenih fazah:

- **Priprava (angl. Pre-engagement)** - pred začetkom aktivnosti je ključno izvesti usklajevalna srečanja z naročnikom in:
    - opredeliti obseg testiranja (angl. scope),
    - določiti jasen cilj (npr. dostop do strežniške sobe, dostop do direktorjeve pisarne, pridobitev zaupnih dokumentov),
    - dogovoriti se o pravilih sodelovanja (angl. rules of engagement) (npr. brez povzročanja škode, časovni okvir testiranja, obveščanje o kritičnih ranljivostih),
    - vzpostaviti varnostne mehanizme, vključno z dokumentom o dovoljenju za testiranje (angl. get out of jail free card), ki ščiti člane ekipe v primeru pravnih ali operativnih zapletov.

- **Izvidništvo (angl. Reconnaissance)** - izvidništvo predstavlja temelj za nadaljnje faze testiranja. Cilj je zbrati čim več informacij o ciljnem objektu brez aktivnega poseganja v okolje. Začne se z uporabo OSINT[17] tehnik, pri čemer se analizirajo:
    - satelitske slike,
    - javno dostopni podatki o objektu (npr. lastništvo, tlorisi, varnostni protokoli),
    - fizična postavitev zgradbe (npr. ograje, vhodi in izhodi, varnostne kamere),
    - objave organizacije in zaposlenih na socialnih omrežjih.

  Na podlagi zbranih informacij črna ekipa načrtuje taktiko in izbere najbolj primerno vrsto izvidništva glede na oddaljenost in zahtevnost dostopa, oddaljeno izvidništvo (angl. long range reconnaissance) ali izvidništvo od blizu (angl. short range reconnaissance) s ciljem pridobiti informacije o:
    - rutini zaposlenih (prihodi in odhodi),
    - pravilih oblačenja (angl. dress code),
    - izgledu dostopnih kartic,
    - lokaciji senzorjev, kamer in drugih zunanjih varnostnih elementov.

  Zaključna faza izvidništva je notranje izvidništvo (angl. embedded reconnaissance), kjer ekipa poskuša pridobiti informacije o notranjosti objekta in zaposlenih z diskretnim, pogosto nevsiljivim vstopom v objekt pri čemer je cilj:
    - identificirati notranje varnostne mehanizme,
    - opazovanje vedenjskih vzorcev zaposlenih (receptorke/ji, tajnice/ki, varnostno osebje),
    - locirati elektronsko nadzorovane prehode,
    - preveriti prisotnost alarmov, notranjih senzorjev, kamer in drugih varnostnih elementov,
    - pridobiti informacije ter vzpostaviti poznanstva s tehnikami socialnega inženiringa.
- **Izraba ranljivosti (angl. Exploitation)** - za izvidništvom sledi faza izrabe identificiranih ranljivosti, kjer črna ekipa na podlagi zbranih informacij aktivno izkoristi odkrite pomanjkljivosti za vdor v ciljni objekt. Namen te faze je pridobiti nepooblaščen dostop do notranjih prostorov in sistemov z izrabo odkritih pomanjkljivosti, na primer:
    - neustrezno zavarovane točke dostopa,
    - uporaba dostopnih kartic, ki jih je možno klonirati,
    - pomanjkljivi postopki preverjanja identitete,
    - ranljive točke v sistemih nadzora dostopa.

  Izraba lahko vključuje uporabo različnih tehnik, kot so:
    - kloniranje dostopnih kartic,
    - manipulacija čitalcev kartic,
    - fizični dostop preko neprimerno varovanih vhodov (npr. preskakovanje preko ali plazenje pod vrati, tailgating, lockpicking),

[17] OSINT - Open Source Intelligence

  - uporaba lažnih identitet ter socialni inženiring za izkoriščanje zaupanja zaposlenih in prehod varnostnih kontrol (npr. novo zaposleni, dostava, pozabljena dostopna kartica).

- **Pridobitev dostopa (angl. Gaining Access)** - po uspešno izvedeni izrabi ranljivosti, sledi pridobitev dostopa v ciljni objekt ali okolje. Poudarek je na neopaženem in nadzorovanem vstopu, ki omogoča izvajanje nadaljnjih aktivnosti brez sprožitve varnostnih mehanizmov. V tej fazi se izvedejo ključni koraki, kot so zbiranje občutljivih informacij, dostop do nezavarovanih naprav ali strežnikov, nameščanje zlonamerne strojne opreme (npr. keylogger, LAN Turtle, Rubber Ducky) ter, če je v obsegu testiranja, vzpostavitev dolgoročne prisotnosti (angl. persistence). Namen te faze ni zgolj vstop, temveč zavzetje ključne pozicije znotraj okolja za nadaljnjo eskalacijo ali preverjanje odpornosti organizacije.
- **Poročanje (angl. Reporting)** - zaključna faza penetracijskega testiranja je priprava podrobnega poročila, ki povzema ugotovitve, izvedene tehnike in odkrite pomanjkljivosti. Poročilo vsebuje oceno tveganj, vplivov na varnost ter priporočila za odpravo ugotovljenih ranljivosti. Pomembno je, da poročilo vključuje tudi vse možne poti dostopa, ki so bile odkrite med fazo izvidništva, čeprav je bila med fazo izrabe ranljivosti preizkušena le ena izmed njih. Ostale poti, ki niso bile neposredno testirane, se v poročilu posebej izpostavijo, da se lahko naročnik sam odloči za njihovo nadaljnjo preizkušnjo ali pa je na njih še posebej pozoren pri izboljševanju varnostnih ukrepov.

  Pomemben del te faze je tudi predstavitev rezultatov naročniku, kjer se razložijo ključni problemi, možni napadi in predlagane izboljšave. Namen poročanja je omogočiti naročniku boljše razumevanje ranljivosti ter zagotoviti izhodišče za izboljšanje varnostnih ukrepov ter zmanjšanje tveganj v prihodnosti.

Fizični varnostni pregledi

Črna ekipa poleg fizičnih penetracijskih testov pogosto izvaja tudi strukturirane fizične varnostne preglede, pri katerih za razliko od penetracijskih testov, člani ekipe ne ohranjajo prikritosti, temveč se lahko odkrito gibljejo po prostorih organizacije ter sistematično prepoznavajo in preverjajo varnostne pomanjkljivosti. V primerjavi s penetracijskim testom, kjer je za dosego cilja testirana le ena izmed vseh odkritih pomanjkljivosti, so pri fizičnem varnostnem pregledu testirane vse odkrite pomanjkljivosti, saj kot že prej omenjeno, člani ekipe ne rabijo paziti na neopaznost. Med fizičnim pregledom se ocenjujejo različni varnostni elementi, kot so:

- analiza sistemov kontrole dostopa (npr. vrsta in možnost kloniranja dostopnih kartic, uporabljeni protokoli, možnost zaobitve vgrajenih sistemov),
- pregled politik za obiskovalce in dobavitelje (npr. vpis v evidenco, določanje spremljevalca, omejen dostop),
- ocenjevanje učinkovitosti fizičnih ovir, alarmov in nadzorne opreme (npr. postavitev kamer in senzorjev, mrtve točke, zaobitev ovir, možnost onesposobitve alarmnih naprav),
- simulacije evakuacij in kriznega odziva,
- stanje in učinkovitost ključavnic in vrat (npr. možnost vdiranja v ključavnice, uporaba orodij za odpiranje vrat od znotraj, zdrs zatiča ključavnice),
- vidnost in odzivnost varnostnega osebja,
- označevanje in nadzorovanje nevarnih ali omejenih območij.

Večina organizacij praviloma na začetku še ni pripravljenih na izvedbo celovitega fizičnega penetracijskega testa, saj pogosto nimajo jasnega pregleda nad lastno fizično varnostno izpostavljenostjo. Zaradi pomanjkanja evidence osnovnih varnostnih kontrol in neustrezne ocene tveganj, cilji testiranja pogosto niso jasno opredeljeni. Nejasno zastavljeni cilji so lahko tudi posledica širših organizacijskih izzivov, kot so pomanjkanje zrelosti varnostne

strategije, odsotnost sodelovanja med ključnimi oddelki (npr. fizično varovanje, IT in poslovno vodstvo), slabo razumevanje metodologije testiranja ali izvajanje testov zgolj zaradi zunanjih zahtev oziroma skladnosti z regulativo in ne zaradi dejanske notranje varnostne potrebe.

Priporočljivo je, da organizacija najprej izvede sistematičen fizični varnostni pregled, v okviru katerega se identificira in dokumentira večje število obstoječih varnostnih pomanjkljivosti. Ta korak omogoča organizaciji, da se seznani s ključnimi tveganji ter pripravi ustrezne ukrepe za odpravo ranljivosti. Šele po implementaciji korektivnih ukrepov je smiselna izvedba fizičnega penetracijskega testa, katerega cilj je preveriti učinkovitost uvedenih izboljšav in odkriti morebitne preostale ranljivosti.

5.2. Vloga fizičnega penetracijskega testiranja v evropski direktivi CER

Evropska direktiva o odpornosti kritičnih subjektov (**CER**[18]**)**, ki je začela veljati decembra 2022 in je morala biti do oktobra 2024 implementirana v zakonodaje držav članic Evropske unije, uvaja obvezne varnostne ukrepe za zaščito **kritične infrastrukture** pred fizičnimi in hibridnimi grožnjami. Med ključnimi novostmi direktive je tudi okrepljen poudarek na **celovitem upravljanju fizične varnosti**, kjer pomembno vlogo dobivajo **realistične simulacije napadov**, vključno z **rednim izvajanjem fizičnih penetracijskih testov**.

Fizični penetracijski testi, kot jih predvideva CER, morajo preverjati odpornost organizacije na napade, ki izvirajo iz fizičnega dostopa do objektov, vključno z nepooblaščenim vdorom, socialnim inženiringom, zlorabo dostopnih točk ter fizičnim izklopom ključne infrastrukture. V kontekstu aktivnosti **črne ekipe** kjer napadalci nimajo vnaprejšnjih informacij ali začrtane poti, takšni testi predstavljajo verodostojno simulacijo realnega tveganja, s katerim se lahko soočajo energetski, prometni, zdravstveni in drugi kritični sektorji.

Zahteve CER tako organizacijam ne nalagajo zgolj formalnega ocenjevanja varnosti, temveč jih zavezujejo k **aktivnemu preverjanju odpornosti** z uporabo metod, ki vključujejo **tako napovedljive kot nepredvidljive napade**, kar predstavlja pomemben korak k bolj proaktivni obrambi. Aktivnosti črne ekipe, v tem okviru, postajajo ena izmed ključnih praks za dokazovanje skladnosti in dejanske pripravljenosti organizacije na fizične grožnje.

5.3. Primeri fizičnih pomanjkljivosti z digitalnimi elementi

Fizični dostop napadalcem omogoča izkoriščanje fizičnih ranljivosti, človeških napak ter neposredno manipulacijo s strojno in omrežno opremo, ki lahko vodi v digitalno kompromitacijo. Gre za napade, kjer napadalec pridobi fizični dostop do naprav, omrežne infrastrukture ali okolja, v katerem lahko nato sproži digitalne vektorje napada, pogosto popolnoma mimo klasičnih varnostnih kontrol. V nadaljevanju predstavljamo primere takšnih napadov, ki vključujejo digitalne komponente in so posledica pomanjkljive zaščite fizične infrastrukture, neustreznih praks ali tehnično zastarelih rešitev. Ti primeri izpostavljajo potrebo po tesnem prepletu fizične in informacijske varnosti znotraj organizacijske varnostne strategije.

Kloniranje dostopnih kartic

Kloniranje dostopnih kartic je ena izmed najpogostejših in najučinkovitejših tehnik fizičnega napada. Številne organizacije še zmeraj uporabljajo starejše RFID[19] tehnologije (npr. 125 kHz HID Prox ali 13.5 MHz MIFARE Classic), ki ne vključujejo osnovne kriptografske zaščite in jih je možno klonirati z uporabo enostavno dostopnih naprav, kot sta Proxmark3 ali Flipper Zero. Napadalec lahko zabeleži signal kartice mimoidočega zaposlenega,

[18] CER - **Critical Entities Resilience**
[19] RFID - Radio-frequency identification

pogosto brez njegove vednosti in brez fizičnega stika, ter ustvari popoln klon, s katerim nato pridobi fizični dostop do zaščitenih območij.

V nasprotju s tem naprednejše kartične tehnologije, kot je MIFARE DESFire EV2/EV3, uporabljajo sodobne kriptografske mehanizme (npr. AES-128), kar bistveno otežuje oziroma onemogoča kloniranje brez dostopa do skrivnih ključev. Žal so takšne rešitve v praksi še zmeraj redkost, bodisi zaradi stroškov bodisi zaradi pomanjkanja ozaveščenosti o tveganjih.

Priporočljiva je opustitev uporabe zastarelih RFID kartic brez kriptografske zaščite ter prehod na varnejše tehnologije, kot so MIFARE DESFire EV2/EV3 ali druge kartice s podporo za AES šifriranje, avtentično dvosmerno komunikacijo ter centralizirano upravljanje ključev. Takšna nadgradnja bistveno zmanjša verjetnost kloniranja in zagotavlja višjo stopnjo zaščite fizičnega dostopa, ki je pogosto prva linija obrambe pred usmerjenimi napadi.

Manipulacija čitalcev kartic

Kljub uporabi varnejših kartičnih tehnologij, še ne pomeni, da je sistem kontrole dostopa varen kot celota. Eden izmed pogosto spregledanih napadov vključuje fizično manipulacijo čitalcev kartic, pri čemer napadalec izpostavi ali prestreže komunikacijo med čitalcem in krmilnikom. Večina starejših sistemov uporablja Wiegand protokol, ki je nekriptiran, enosmeren in ranljiv za pasivno prisluškovanje, ponavljanje prenosa (angl. replay attack) ali celo manipulacijo podatkov.

Napadalec lahko s fizičnim dostopom do ožičenja čitalca (npr. zunaj stavbe ali v slabo varovanem hodniku) priključi napravo, ki beleži ali posreduje podatke o avtorizaciji. V določenih primerih je mogoče s pomočjo preprostega napada reproducirati signal in tako simulirati legitimno kartico brez njene prisotnosti.

Priporočljiva je uporaba kriptografsko zaščitenih protokolov, kot so OSDP[20] s podporo za AES šifriranje in dvosmerno preverjanje pristnosti. Poleg tega je potrebno zagotoviti fizično zaščito komunikacijskih poti med čitalci in krmilniki (npr. uporaba oklopljenih vodnikov ali zaznava fizične manipulacije čitalcev kartic) ter spremljanje nenavadnih dogodkov v sistemu dostopa.

Prekomerne pravice dostopa

Pogosta, a večkrat spregledana ranljivost je dodeljevanje preširokih dostopnih pravic znotraj sistemov kontrole dostopa. V številnih organizacijah imajo zaposleni ali pogodbeni delavci dostop do večjega števila prostorov, kot jih dejansko potrebujejo za svoje delo. Napadalec, ki pridobi klonirano kartico takšne osebe, lahko brez omejitev vstopi v občutljive prostore, kot so strežniške sobe, arhivi ali tehnični prostori, kjer ima neposreden dostop do informacijskih sistemov, omrežne opreme ali dokumentacije.

Poleg očitnega povečanja varnostnega tveganja takšna ureditev otežuje tudi revizijsko sledenje in odziv v primeru incidenta, saj dostop ni omejen glede na dejanske potrebe uporabnika.

Priporočljivo je dosledno uveljavljanje načela najmanjšega potrebnega dostopa (angl. least access) v okviru sistemov kontrole dostopa. Vsaka dostopna pravica naj bo dodeljena na podlagi konkretnih delovnih nalog in preverjena ob spremembi zaposlitve, vloge ali lokacije dela. Na ta način morebitni nepooblaščeni fizični vdori ne ogrozijo celotne organizacije, temveč ostanejo omejeni na najmanjši možni obseg, kar bistveno zmanjša varnostno tveganje.

[20] OSDP - Open Supervised Device Protocol

Nenadzorovani in odklenjeni računalniki

Ena pogostejših napak zaposlenih je puščanje odklenjenih računalnikov brez nadzora. V času kratke odsotnosti uporabnika, lahko napadalec z dostopom do delovne postaje priključi zlonamerno napravo (npr. Rubber Ducky ali Bash Bunny), ki je ob priklopu v računalnik prepoznana kot vhodna periferna naprava (tipkovnica, miška, ipd.) in samodejno izvede preddefinirane sistemske ukaze ter skripte brez uporabnikove interakcije. S tem lahko napadalec že v nekaj sekundah pridobi nadzor nad sistemom.

Priporočljivo je dosledno uveljavljanje politike samodejnega zaklepanja zaslona po krajšem obdobju neaktivnosti (npr. 3-5 minut) ter ozaveščanje zaposlenih, da ob vsaki odsotnosti zaklenejo delovno postajo. Poleg tega je priporočljiva omejitev uporabe administrativnih privilegijev pri rednem delu in kontrola priklopa perifernih naprav.

Varnostne ranljivosti videonadzornih sistemov

Videonadzorni sistemi (CCTV[21]) predstavljajo ključen steber fizične varnosti, a obenem tudi pogosto spregledano točko napada, če niso ustrezno fizično in logično zaščiteni. Ena izmed najpogostejših ranljivosti je nezaščiteno ožičenje, ki je pogosto lahko dostopno (npr. nad spuščenimi stropi ali ob fasadah), kar omogoča fizične posege npr. prekinitve, preusmeritve ali celo vključitev zlonamernih naprav. Prav tako lahko IP-kamere, povezane na slabo segmentirano omrežje, služijo kot izhodišče za vstop v IT okolje organizacije.

Druga kritična pomanjkljivost je neoptimalna postavitev kamer, ki ustvarja slepe točke, kjer se lahko napadalec giblje ali izvaja dejavnosti brez nadzora. V praksi se črne ekipe pogosto poslužujejo vstopov skozi servisne vhode, kletne garaže ali izkoriščanja mrtvih kotov ob kamerah, ki niso ustrezno usmerjene ali se prekrivajo s slepimi območji drugih kamer. Poleg tega so kamere pogosto nameščene na dosegljivih mestih brez zaščite proti fizičnim posegom, kar omogoča njihovo obračanje, prekrivanje ali mehansko poškodbo, brez sprožitve alarma.

Za učinkovit videonadzor je potrebno več kot le prisotnost kamer. Priporočljiva je:

- uporaba oklopljenih in skritih vodnikov,
- aktiviranje zaznave fizičnih posegov,
- ločena omrežna segmentacija IP-kamer,
- redni pregledi in testiranja vizualnega pokritja za odpravo slepih točk,
- vključitev videonadzornih sistemov v redne fizične penetracijske teste.

Kamera, ki je fizično ali logično ranljiva, ne le izgubi svojo varovalno funkcijo, temveč lahko postane tudi vektor napada zoper organizacijo samo.

6 Sodelovanje med ekipami

Med aktivnostmi črne in rdeče ekipe lahko potegnemo določene vzporednice. Tako pri digitalnem penetracijskem testiranju kot pri fizičnem varnostnem pregledu je cilj široko zastavljen: identificirati čim več ranljivosti v obravnavanem sistemu ali okolju. Gre za celovit pregled, katerega namen je zagotoviti temeljito razumevanje varnostne izpostavljenosti organizacije.

Za razliko od tega pa imata fizično penetracijsko testiranje in red teaming aktivnosti jasno definirane cilje. Ti vključujejo preverjanje možnosti doseganja konkretnega cilja, kot je na primer nepooblaščen dostop do strežniške sobe ali dostop do zaupnih dokumentov. V tem kontekstu izvajalci testiranja običajno ne preverjajo drugih

[21] CCTV - Closed-circuit television

priložnostnih ranljivosti, kot so denimo prost dostop do direktorjeve pisarne ali dostop do varnostnih kopij občutljivih sistemov - razen če so takšni cilji vnaprej opredeljeni v obsegu testa.

Najuspešnejši napadi pogosto združujejo prepletenost aktivnosti rdeče in črne ekipe. V simulacijah lahko črna ekipa najprej izvede fizični vdor, nato pa iz notranjega omrežja sproži kibernetski napad kjer rdeča ekipa nadaljuje z identifikacijo in izkoriščanjem digitalnih pomanjkljivosti. Takšna integracija je ključna za testiranje realne odpornosti organizacije na kompleksne napade in omogoča realno presojo, ali obrambni sistemi (modra ekipa) zaznajo tako kompleksne grožnje.

Po končanih simulacijah lahko vijolična ekipa deluje kot posrednik in optimizator, ki povezuje opažanja črne, rdeče in modre ekipe ter pomaga prenesti ugotovitve v varnostne izboljšave.

7 Zaključek

Čeprav so v središču sodobnih varnostnih razprav večinoma digitalni napadi, fizična varnost ostaja ključna, a pogosto spregledana komponenta celostne kibernetske obrambe. Črna ekipa ponuja redko priložnost za etično in realistično preverjanje fizičnih obrambnih mehanizmov, ki jih digitalne analize ne morejo zajeti. Takšne simulacije razkrivajo pomanjkljivosti, ki jih standardni tehnični pregledi pogosto spregledajo, zlasti na ravni človeškega faktorja, organizacijske discipline in fizične dostopnosti.

Z vključevanjem črne ekipe v redne varnostne preglede lahko organizacije:

- Okrepijo celostno odpornost na napade vseh vrst.
- Prepoznajo in ublažijo ranljivosti, povezane s socialnim inženiringom, notranjimi grožnjami in fizičnim dostopom.
- Spodbujajo sodelovanje med IT-jem, fizičnim varovanjem in poslovnim vodstvom.
- Uskladijo varnostno prakso z aktualnimi regulatornimi zahtevami.

Še posebej pomembno je to za sektorje z visokim tveganjem kot so finančne ustanove, energetika, zdravstvo, obrambni sistemi in kritična infrastruktura, kjer je lahko že ena sama spregledana pomanjkljivost usodna.

Poleg tega je z uveljavitvijo evropske direktive CER skupaj z direktivo NIS2, postalo zakonsko obvezno, da organizacije, ki sodijo med kritične subjekte, izvajajo ukrepe za zaščito tudi pred fizičnimi grožnjami. To vključuje testiranje ranljivosti na fizični ravni, kar črna ekipa omogoča na varen, strukturiran in neinvaziven način. Neupoštevanje teh zahtev pa ne pomeni le povečane izpostavljenosti tveganjem, temveč tudi regulatorne in finančne posledice.

Celostna kibernetska varnost se ne konča pri požarnih zidovih in geslih - njen resnični preizkus se zgodi, ko nekdo fizično prestopi prag. In prav zato postaja vloga črne ekipe nepogrešljiv del sodobnega varnostnega ekosistema.

Literatura

[1] Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Federick, Ronald W. Ritchey, »Inside Network Perimeter Security«, New Riders Publishing, 2023.

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf, NIST SP 800-61r3 - Incident Response Recommendations and Considerations for Cybersecurity Risk Management, obiskano 9.6.2025.

[3] https://attack.mitre.org, MITRE ATT&CK Framework - Adversarial Tactics, Techniques, and Common Knowledge, obiskano 9.6.2025.

[4] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf, NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment, obiskano 10.6.2025.

[5] https://www.isecom.org/OSSTMM.3.pdf, OSSTMM (ISECOM), »Chapter 8 - Physical Security Testing«, obiskano 10.6.2025.

[6] https://www.iso.org/standard/27001, ISO/IEC 27001:2022, obiskano 10.6.2025.

[7] https://www.iso.org/standard/75652.html, ISO/IEC 27002:2022, obiskano 10.6.2025.

[8] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, NIST SP 800-53r5 - Security and Privacy Controls for Information Systems and Organizations, obiskano 14.6.2025.

[9] https://www.atomicredteam.io, Atomic Red Team, obiskano 19.6.2025.

[10] https://caldera.mitre.org, MITRE Caldera, obiskano 19.6.2025.

[11] https://www.enisa.europa.eu/sites/default/files/2024-11/Implementation%20guidance%20on%20security%20measures_FOR%20PUBLIC%20CONSULTATION.pdf, ENISA Implementing Guidance - Environmental And Physical Security, obiskano 21.7.2025.

[12] https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20-%20Guideline%20on%20Security%20Measures%20under%20the%20EECC-%204th%20edition.pdf, ENISA Guideline On Security Measures Under The EECC - D3: Security of systems and facilities, obiskano 21.7.2025.