REKOMENDACIJOS, KAIP SUORGANIZUOTI IMITACINES SOCIALINĖS INŽINERIJOS PRATYBAS

Imitacinės socialinės inžinerijos pratybos – tai kibernetinio saugumo pratybų tipas, taikomas kaip viena iš saugumo supratimo (angl. *security awareness*) mokymų dalių. Šios pratybos skirtos organizacijos personalo kibernetinio saugumo supratimui ir gebėjimui atpažinti galimas grėsmes ugdyti, patikrinti, ar darbuotojas žino, kokių veiksmų turi imtis gavęs įtartiną el. laišką, SMS žinutę ar pan..

Nacionalinis kibernetinio saugumo centras (toliau – NKSC) ragina organizacijas nuolatos ugdyti savo darbuotojų atsparumą kibernetinėms grėsmėms ir periodiškai organizuoti įvairias pratybas, tarp kurių turėtų būti ir imitacinių socialinės inžinerijos atakų. Kokybiškai mokymo tikslais įgyvendintos tokios „atakos“ yra panašios į tikrąsias sukčių atakas, todėl jų panaudojimas be išankstinio koordinavimo su kitomis susijusiomis arba potencialiai paveikiamomis institucijomis gali sutrikdyti veiklą tiek pratybas vykdančios organizacijos viduje, tiek ir išorinėse organizacijose. Todėl NKSC ragina visus pratybų organizatorius atsakingai jas planuoti ir pateikia rekomendacijas, kaip saugiai organizuoti imitacines socialinės inžinerijos pratybas savo darbuotojams.

SUDERINIMAS SU SUINTERESUOTOMIS ŠALIMIS

Imitacinių socialinės inžinerijos pratybų tikslas yra patikrinti darbuotojų atsparumą duomenų viliojimo atakoms, kurios gali būti vykdomos įvairiais būdais: klastojant el. laiško (angl. *phishing* ataka), SMS žinutės (angl. *smishing* ataka), ar skambinančiojo (angl. *vishing* ataka) asmens tapatybę.

Ilgametė NKSC pratybų organizavimo patirtis rodo, kad dalis sąmoningų darbuotojų apie gautus įtartinus el. laiškus informuoja ne tik savo organizacijos kibernetinio saugumo specialistą, bet ir kitas valstybės institucijas, todėl prieš pradėdami vykdyti tokias pratybas, iš anksto informuokite susijusias institucijas ir asmenis, gaukite jų sutikimą.

Prieš pratybų pradžią rekomenduojame:

1. Gauti išankstinį raštišką organizacijos, kurios logotipas, domenas ar prekinis ženklas bus naudojamas pratybose, sutikimą. Jo reikia ir tais atvejais, kai planuojama naudoti panašius ir tikruosius prekės ženklus imituojančius pavadinimus (pvz., „VM1“ vietoj „VMI“).
2. Iš anksto raštiškai su savo organizacijos atstovu, atsakingu už informacijos saugumą, suderinti, kad būtų galima atlikti sukčiavimą imituojančius veiksmus naudojant konkrečius šablonus.

3. Prieš 3 darbo dienas el. paštu cert@nksc.lt informuoti NKSC apie planuojamas pratybas, nurodyti pradžios ir pabaigos datą ir laiką, pateikti planuojamo naudoti el. laiško šablono pavyzdį.

ĮRANKIAI (PRODUKTAI)

Imitacinėms pratyboms galima naudoti įvairius komercinius įrankius ar produktus, skirtus duomenų viliojimo (angl. *phishing*) atakoms vykdyti. Juose dažniausiai pateikiami šablonai, imituojantys trečiųjų šalių („Google“, „Microsoft“, „Apple“ ir kt.) domenų vardus, prekinius ženklus ir logotipus. Atkreipiame dėmesį, kad toks trečiųjų šalių nuosavybės panaudojimas gali pažeisti subjektų prekės ženklo ar autorių teises.

Analogiška nuostata galioja ir norint naudotis Lietuvos bendrovių ar institucijų (pvz., Valstybinės mokesčių inspekcijos, „Sodros“, NKSC ir t. t.) šablonais, vardais, domenais ar logotipais. Todėl organizacija, planuojanti pratybas, privalo gauti atskirą imituojamų organizacijų leidimą naudoti jų prekės ženklus arba naudoti aiškiai matomus pranešimus (angl. *disclamers*), informuojančius vartotojus, kad organizacijų logotipai, prekiniai ženklai naudojami tik mokymo tikslais.

Renkantis komercinius įrankius, ypatingą dėmesį reikėtų atkreipti į duomenų apsaugą, taip pat užtikrinti, kad per pratybas nebūtų renkami pertekliniai duomenys. Pratybų dalyvių turi būti prašoma pateikti tik tiek duomenų, kiek jų reikia kibernetinio saugumo žinioms patikrinti. Surinkti duomenys turėtų būti vertinami anonimiškai. Pratyboms reikėtų rinktis tuos produktus, kurių kūrėjai yra deklaravę savo produkto atitiktį Europos Sąjungos Bendrojo duomenų apsaugos reglamento (ES BDAR) reikalavimams, duomenis apdoroja ir saugo Europos Sąjungos teritorijoje, yra aiškiai apibrėžę ir paskelbę duomenų subjektų teises.

Pratyboms galima ir specialiai įsigyti atskirus domenus. Tokiu atveju per pratybas naudojami domenų vardai turi būti registruojami nurodant pratybas vykdančios organizacijos kontaktinę informaciją, kad kitos išorinės organizacijos, netyčia gavusios pranešimus apie pastebėtus įtartinus laiškus, galėtų greičiau nustatyti tikruosius pratybų organizatorius.

PRATYBŲ PLANAS

Pratybų planas – tai iš anksto parengtas dokumentas, skirtas sklandžiam pratybų vykdymui, koordinacijai su išorinėmis organizacijomis, kontrolei užtikrinti, auditorijai ir turiniui numatyti.

Minimalus pratybų planas:

1. Pratybų vykdymo laikotarpis ir jų periodiškumas. Pratybos gali būti vienkartinės arba vykti periodiškai (kas dvi savaites, kas mėnesį, kas ketvirtį, kas metus).
2. Auditorija. Pratybos gali būti skirtos visiems arba tik tam tikriems organizacijos darbuotojams.
3. Turinys. Suklastotuose el. laiškuose naudojami subjektų pavadinimai, prekės ženklų ir logotipų maketai.
4. Pranešimai treniruojamai auditorijai. Dalyvius rekomenduojama informuoti prieš pratybas ir po jų.
5. Suderinimas su suinteresuotomis šalimis. Išorines organizacijas ir savo organizacijos personalą, kuriems vykdomos pratybos gali turėti poveikį, rekomenduojama informuoti iš anksto (žr. skyrių „Suderinimas su suinteresuotomis šalimis“).
6. Pratybų kontrolė. Paskiriamas už pratybų vykdymą atsakingas asmuo, nurodomi jo tiesioginiai kontaktai, išvardijami veiksmai, kurių jis imsis siekdamas tinkamai valdyti pratybas.
7. Stebėtojai. Paskiriami asmenys, kurie stebės pratybų eigą ir (ar) taikomosios programinės įrangos žurnalų įrašus.
8. Metrikos ir duomenys. Aprašomi kiekybiniai požymiai, pagal kuriuos bus vertinamas pratybų dalyvių elgesys (pvz., atidarė el. laišką, paspaudė kenksmingą nuorodą, informavo atsakingus asmenis organizacijos viduje ir pan.). Aprašoma, kaip bus tvarkomi per pratybas iš dalyvių surinkti duomenys, kad būtų laikomasi ES BDAR reikalavimų.

VIDINĖ KOORDINACIJA IR KONTROLĖ

Glaudus bendradarbiavimas ir koordinacija su kitais organizacijos padaliniais ir išorinėmis organizacijomis, kurios gali būti paveiktos pratybų, užtikrina sėkmingą pratybų vykdymą ir kontrolę pagal iš anksto sudarytą planą.

Koordinacija su organizacijos vidiniais padaliniais (informacinių technologijų (IT) saugos padalinys, pagalbos tarnyba, administratoriai) turi vykti tiek planuojant pratybas (pvz., gaunant pratyboms vykdyti reikalingus leidimus, vykdant išankstinius darbuotojų mokymus apie veiksmus gavus įtartiną laišką ir pan.), tiek ir jų metu (pvz., pagalbos tarnybai padedant atsakyti į per pratybas darbuotojų pateiktas užklausas).

Imituojant realias grėsmes, su kuriomis susiduria organizacijos, svarbu užtikrinti realią darbuotojų patirtį saugioje aplinkoje. Tai pasiekti padeda iš anksto aptarti ir įdiegti baziniai kontrolės sprendimai ir glaudi pratybų vykdytojų koordinacija su:

- organizacijos IT saugos komanda, kuri turi užtikrinti pratybose naudojamų el. laiškų pralaidumą per brukalo gaudykles ir kitus filtravimo mechanizmus ir siunčiamų el. laiškų srauto ribojimą, kad pratybų el. laiškai nebūtų persiunčiami už iš anksto nustatytų pratybų auditorijos ribų;
- organizacijos pagalbos tarnyba (angl. *helpdesk*) atsakant į darbuotojų užklausas (pagalbos tarnybai informacija teikiama iš anksto);
- organizacijos IT administratoriais pašalinant pratybų el. laiškus iš darbuotojų el. pašto dėžučių, bendrinamųjų pašto dėžučių ar kitų pratybų paveiktų informacijos saugyklų.

TURINYS IR METRIKOS

Siekiant užtikrinti dalyvių privatumą, pratybų turinį turi sudaryti tik viešai prieinama informacija. Pratybų vykdytojai negali turėti galimybės rinkti asmeninius duomenis (pvz., slaptažodžių, vardų, pavardžių, telefono numerių, banko kortelės numerių ir pan.). Imitacinės pratybų svetainės privalo būti sukurtos taip, kad žiniatinklio serveriui niekada nebūtų pateikta informacija (vartotojų pateiktos formos duomenys atmetami prieš juos pateikiant). Taip pat, kuriant turinį, svarbu užtikrinti, kad per pratybas nebūtų naudojama netinkama ar jautri informacija ir kad politinių partijų, organizacijų pavadinimai, bendrovių pavadinimai ir (ar) jų logotipai nebūtų naudojami be išankstinio raštiško tų bendrovių sutikimo.

Vykdant pratybas rekomenduojama fiksuoti:

- bendrą el. laišką atsidariusių darbuotojų skaičių;
- bendrą darbuotojų, paspaudusių nuorodą el. laiške, skaičių;
- bendrą darbuotojų, įvedusių reikalaujamus duomenis imituojamoje svetainėje, skaičių;
- bendrą darbuotojų, atidariusių neva kenksmingą priedą ar aktyvavusių neva kenkimo programą, pateiktą imituojamoje svetainėje, skaičių;
- bendrą darbuotojų, apie pastebėtą įtartiną laišką pranešusių organizacijos kibernetinio saugumo specialistui ar pagalbos tarnybai (angl. *helpdesk*), skaičių.

Jeigu pratybos yra organizuojamos periodiškai, rekomenduojama rengti lyginamąją metinę suvestinę, kuri parodytų pratybų dalyvių sąmoningumo ugdymo programos brandą ir vykdytos kampanijos efektyvumą.

LITERATŪROS SĄRAŠAS

1. Bell, K. (2020). *GoDaddy phishing 'test' teased employees with a fake holiday bonus*. Nuskaityta iš https://www.engadget.com/godaddy-sent-fake-phising-email-promising-holiday-bonus-220756457.html
2. CDT (2021). *Phishing Exercise Standard SIMM 5320-A.* Nuskaityta iš https://cdt.ca.gov/wp-content/uploads/2020/10/SIMM5320-A-Phishing-Exercise-Standard_2020-0930.pdf
3. Fabio Rizzoni, S. M. (2022). *Phishing simulation exercise in a large hospital: A case study.* Nuskaityta iš https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8935590/
4. Kristen K. Greene, M. P. (be datos). *User Context: An Explanatory Variable in Phishing Susceptibility.* Nuskaityta iš https://www.ndss-symposium.org/wp-content/uploads/2018/07/usec2018_01-2_Greene_paper.pdf
5. Ponnurangam Kumaraguru, J. C. (be datos). *School of Phish: A Real-World Evaluation of Anti-Phishing Training.* Nuskaityta iš https://www.heinz.cmu.edu/~acquisti/papers/Acquisti_Real-World_Evaluation_of_Anti-Phishing_Training.pdf
6. Sevilla, A. (2021). *Many companies would sack employees over phishing mistakes*. Nuskaityta iš https://www.itproportal.com/news/many-companies-would-sack-employees-over-phishing-mistakes/
7. Sosafe. *Best Practices for Phishing Simulations.* Nuskaityta iš https://lp.sosafe.de/hubfs/8858700/SoSafe%20-%20White%20Paper%20-%20Best%20Practice%20Phishing%20Simulation_EN.pdf