"IT higiena ir saugumas – ką galima greitai ir paprastai įgyvendinti organizacijose"



*Lektorius **Tadas Vasiliauskas** – IT vadovas ir praktikas, turintis ilgametę patirtį IT infrastruktūros, „Microsoft 365“, kibernetinio saugumo, sistemų administravimo ir organizacijų skaitmenizavimo srityse.*

Programa:

1. Slaptažodžių politika be skausmo:
    - Kaip keitėsi slaptažodžių politikos.
    - Slaptažodžių naudojimas išorinėse sistemose.
    - Šių dienų moderni autentifikacija ir politikų rekomendacijos.
    - Slaptažodžių dalinimasis ir kaip tai daryti tiesingai.
2. Darbo vietos saugumas per 15 min.:
    - Kokius įpročius reikia išsiugdyti.
    - Kokie baziniai nustatymai turi būti vienodi visose darbo vietose.
    - Kas yra raudonos vėliavos: lėtėjimas, keisti langai, neaiškūs pranešimai.
    - Kada jau reikia kreiptis į IT.
3. El. pašto higiena ir phishing atpažinimas:
    - Kaip atrodo tipiškas phishing laiškas šiandien.
    - Pavojingi priedai, nuorodos ir prisijungimo langai.
    - Kaip tikrinti siuntėją ir laiško kontekstą.
    - Kaip atpažinti skubos, baimės ir „autoriteto“ manipuliaciją.
    - Ką daryti, jei jau paspaudžiau.
4. Prieigų valdymas „kas kam tikrai reikia“:

- Kodėl pavojinga palikti „visiems viską“.
- Naujo darbuotojo, pareigų pasikeitimo ir išėjimo scenarijai.
- Kaip suvaldyti bendras pašto dėžutes, bendrus prisijungimus, bendrus failus.
- Periodinė prieigų peržiūra.
- Kas turi tvirtinti prieigas.
- Šių dienų prieigų administravimas.

5. Failų ir duomenų tvarka (share’ai, debesys):
    - Kur turi gyventi dokumentai: kompiuteryje, serveryje ar debesyje.
    - Pavadinimų, versijų ir aplankų logika, Meta duomenys.
    - Kaip sumažinti „neberandu failo“ problemą.
    - Perteklinis dalinimasis ir viešos nuorodos.
    - Prieigos prie failų iš išorės.
    - Kaip apsaugoti jautresnius dokumentus.
    - Kokias taisykles verta nusistatyti organizacijoje.
6. Atsarginės kopijos: paprastas modelis:
    - Kas iš tikrųjų yra atsarginė kopija, o kas nėra.
    - Kodėl sinchronizacija dar nėra backup.
    - Kiek organizacijai kainuoja „neturime kopijos“ – kas yra „šalta kopija”.
    - Kodėl svarbu periodiškai testuoti atsarginę kopiją.
    - Atsarginių kopijų politikos.
7. Programinės įrangos higiena:
    - Kodėl pavojinga naudoti senas programas.
    - Nemokamų įrankių rizikos.
    - Naršyklės plėtinių, PDF įrankių, nuotolinio prisijungimo programų pavojai.
    - Shadow IT mažinimas organizacijoje.

- Ką būtina standartizuoti.

8. Mobilūs įrenginiai ir nuotolinis darbas:
    - Telefonas kaip pilnavertė organizacijos prieiga.
    - Ekrano užraktas, PIN, biometrika.
    - Nuotolinio darbo rizikos ir bazinės apsaugos priemonės.
    - Kokius minimalius reikalavimus verta taikyti telefonams ir nešiojamiems kompiuteriams.
    - Kaip užtikrinti prieigų saugumą dirbant iš skirtingų vietų.
9. Greitas IT rizikų „self-check“ organizacijai:
    - Kaip atskirti kritines, vidutines ir mažas rizikas.
    - 10 klausimų organizacijos savitikrai.
    - Kaip iš rezultatų sudaryti veiksmų planą.
10. Incidentų mini-planas: ką daryti „kai nutinka“:
    - Kaip suprasti, kad incidentas jau įvyko.
    - Rolės ir atsakomybės.
    - Kaip izoliuoti problemą nepabloginant situacijos.
    - Kodėl svarbu greitis, bet ne panika.
    - Po-incidentinis aptarimas ir pamokos.
11. Darbuotojų elgesio taisyklės (IT higienos kultūra):
    - Kodėl saugumas yra kasdieniai įpročiai, o ne vien IT problema.
    - Kaip kurti atsakingą elgesį be perteklinių draudimų.
    - Kokios 10 taisyklių turi būti aiškios visiems.
    - Kaip neformalūs „išimtiniai atvejai“ naikina politikų veikimą.
12. TOP 10 klaidų, kurias daro organizacijos.

4 akad. val.