ABC INFORMACIJOS APSAUGOS

12 skaidrė:

Kas atsakingas už įslaptintos informacijos saugumą?

- Kiekvienas Jūsų asmeniškai atsakote už Jums patikėtos ar Jūsų rengiamos įslaptintos informacijos saugumą.
- Konsultuotis ir prašyti pagalbos nėra gėda – visada žinokite atitinkamų saugumo pareigūnų ar informacinių technologijų specialistų kontaktus.
- Apie bet kokius kompiuterių sistemų, kitos techninės ar programinės įrangos pasikeitimus ir anomalijas bei saugumo incidentus nedelsdami informuokite informacinių technologijų specialistą ar saugumo pareigūną.
- Įslaptintos informacijos praradimas, atskleidimas ir netinkamas darbas su ja yra teisės pažeidimai ir užtraukią baudžiamąją, administracinę ir tarnybinę atsakomybę.

Pastebėjus sistemingus įslaptintos informacijos apsaugos pažeidinėjimus, kreiptis į AOTD prie KAM:

+370 659 52626 arba **+370 659 06352**

Įvykus incidentui KAS kompiuterių sistemose, kreipkitės į RIST prie KAM Kibernetinio saugumo skyrių:

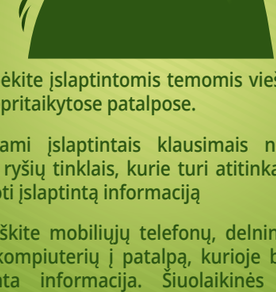
KATT **25 599** arba **(8 37) 307 699**

cert@mil.lt

http://cert.mil.lt

8 skaidrė:

Bendrieji patarimai dirbant su įslaptinta informacija



- Dirbkite su įslaptinta informacija tik tam skirtose patalpose ir kompiuteriuose.
- Net ir trumpam pasitraukę iš darbo vietos, įjunkite slaptažodžiu apsaugotą kompiuterio ekrano užsklandą ir palikite visą įslaptintą informaciją seife arba metalinėje spintoje.
- Sunaikinkite tas dokumentų kopijas, projektus, juodraščius ar užrašus, kurie daugiau nebus naudojami.
- Visada suteikite tinkamą slaptumo žymą.
- Įslaptintą informaciją saugokite seifuose ar metalinėse spintose.
- Vadovaukitės principu „Būtina žinoti“.
- Jei patalpoje, kur Jūs dirbate su įslaptinta informacija, lankosi kiti asmenys, nepalikite tos patalpos be priežiūros.

Kaip užbaigti darbo dieną?

- Susitvarkykite stalą, kad nepaliktumėte įslaptintos ar kitokios „jautrios“ informacijos.
- Įslaptintą informaciją užrakinkite seifuose arba metalinėse spintose.
- Išjunkite kompiuterius, uždarykite langus, užrakinkite duris ir, jei yra, įjunkite signalizaciją.

11 skaidrė:

Kaip saugiai dalytis įslaptinta informacija?

- Nekalbėkite įslaptintomis temomis viešose vietose ir tam nepritaikytose patalpose.
- Kalbėdami įslaptintais klausimais naudokitės tik tokiais ryšių tinklais, kurie turi atitinkamus leidimus perduoti įslaptintą informaciją
- Nesineškite mobiliųjų telefonų, delninių ar nešiojamųjų kompiuterių į patalpą, kurioje bus aptariama įslaptinta informacija. Šiuolaikinės technologijos leidžia nuotoliniu būdu pasiklausyti pokalbių, įrašyti vaizdinę medžiagą ir kopijuoti Jūsų telefone saugomus duomenis.

9 skaidrė:

Pasitikrinkite žinias

1. Kompiuterių tinklas, kurį sukuria kenkėjiška programa, taip sudarydama sąlygas vykdyti atakas, valdomas iš išorės. **2.** Principas „..... žinoti“. **3.** Kas yra atsakingas už Jums patikėtos ar rengiamos įslaptintos informacijos saugumą? **4.** Į ką, įvykus incidentui KAS kompiuterių sistemose, reikėtų kreiptis? **5.** Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo raidinė santrumpa. **6.** Koks disponavimas įslaptinta informacija, kuri yra valstybės paslaptis, užtraukia baudžiamąją atsakomybę? **7.** Viena iš vietų, kur turi būti laikoma įslaptinta informacija pasibaigus darbo valandoms. **8.** Kokių siuntėjų laiškų nerekomenduojama atidaryti? **9.** Atsakomybė, kurią užtraukia įslaptintos informacijos praradimas. **10.** Viena iš viešų elektroninio pašto sistemų, kuri neturi būti naudojama tarnybinei informacijai siųsti. **11.** Nestabilus kompiuterio darbas, iššokantys langai, reklamos – šie požymiai leidžia įtarti, kad kompiuteris užkrėstas ... **12.** Saugesnio ryšio su interneto puslapiais protokolą nurodančios raidės puslapio adreso pradžioje.

3 skaidrė:

7 skaidrė:

Ar žinote, kad...

? Siūlytina internete nenurodyti tiesioginio elektroninio pašto adreso **Vardas@example.com.** Geriau adresą užrašykite taip, kad jis būtų žmogui lengvai suprantamas, tačiau klaidintų kompiuterio programą, surenkančią tokius duomenis.
Geriau rašykite taip, kaip sakytumėte žodžiu:
Vardas+ETA+example+DOT+com.

? Prieš registruodamiesi tinklalapyje, kuriame pateiksite savo konfidencialius duomenis (tarkim, el. bankininkystė), įsitikinkite, ar puslapio adresas prasideda **„http://“ ar „https://“**. Raidė „s“–„secure“ reiškia, kad ryšio sesija su tuo serveriu, su kuriuo bendraujate, yra apsaugota.
Taigi patikimesnis puslapio adresas yra https:// .

? Netikėtai iššokančius langus (*pop-up*) uždarykite spausdami **ne „Cancel“ ar „No“**, o paspausdami ženkliuką **„X“** arba klavišų kombinaciją **„Alt + F4“**.
Paspaudus „Cancel“ ar „No“, gali būti suaktyvinama kenkėjiška programa Jums to net nepastebint.

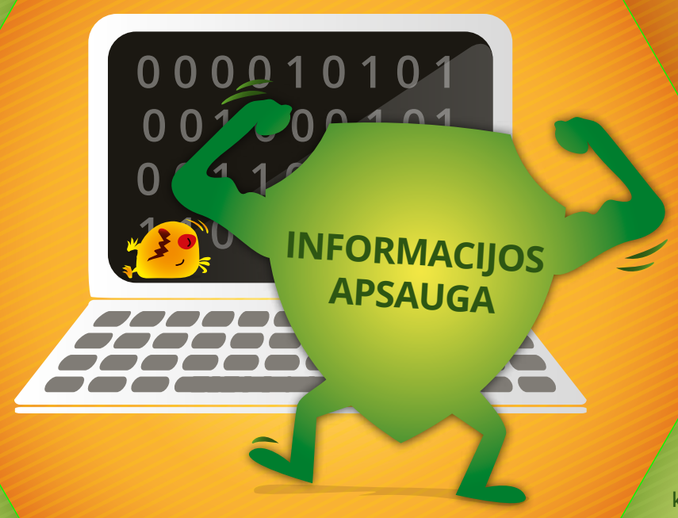
? Siųsdami laiškus keliems gavėjams vienu metu, jų adresus rašykite į **„Bcc“** laukelį. Taip gavėjai nematys vienas kito ir jų kompiuteriuose esančios programos nefiksuos adresų.

6 skaidrė:

Kokie požymiai leidžia įtarti, kad kompiuteris gali būti užkrėstas virusu?

- Nuolatinis / labai ilgai trunkantis standžiojo disko darbas
- Besikeičiantys operacinės sistemos ir kitų programų nustatymai
- Kitomis aplinkybėmis pastebite, kad Jūsų duomenys galėjo būti atskleisti
- Sutrikęs antivirusinės programos darbas
- Automatiškai pasileidžiančios programos
- Nukreipimas į keistus interneto puslapius
- Iššokantys langai, reklamos
- Sulėtėjęs ar nestabilus kompiuterio darbas

SVARBU!
Šiuolaikinės šnipinėjimo programos tokių išskirtinių požymių, kurie padėtų pastebėti pakitusią Jūsų kompiuterio veiklą, neturi.



ATSIMINKITE, KAD INFORMACIJOS SAUGUMAS PRIKLAUSO TIK NUO JŪSŲ!

4 skaidrė:

Kas ir koks yra kibernetinis šnipinėjimas?

- Kibernetinis šnipinėjimas – tai tikslinga veikla, skirta surinkti reikiamą informaciją naudojant kompiuterių sistemas ir kibernetinę erdvę.
- Kibernetinį šnipinėjimą gali vykdyti valstybės ar valstybių remiami kibernetiniai agresoriai, taip pat ir kiti kibernetiniai agresoriai, veikiantys ne valstybių užsakymu.
- Šiuo metu Lietuvoje aptinkama šnipinėjimo programa, skirta rinkti kompiuteryje esančius duomenis, valdyti užkrėstą kompiuterį nuotoliniu būdu, stebėti tinklą, identifikuoti tinkle esančias paskyras ir slaptažodžius.
- Šnipinėjimo programa dažniausiai plinta per išorines USB laikmenas, optinius (CD ir DVD), standžiuosius (HDD) diskus ir su elektroninių laiškų priedais.
- Šnipinėti skirta programa gali aktyvuoti kompiuteryje esančią vaizdo kamerą ar mikrofoną ir vykdyti pasiklausymą realiuoju laiku.
- Lietuvoje žinoma dar viena aptiktos šnipinėjimo programos funkcija, kurianti kompiuterių tinklą „BotNet“ , kuris sudaro sąlygas nuotoliniam kompiuterių valdymui. Paprastai tokio tinklo pagrindinė paskirtis – kibernetinės atakos.
- Šnipinėti skirta programa nuolat modifikuojama ir papildoma naujomis funkcijomis. Kai kurios versijos numato savaiminį kenkėjiškos programos susinaikinimą išsiuntus informaciją.

Įprastinės antivirusinės programos šios šnipinėjimo programos neaptinka.

5 skaidrė:

Kaip saugotis virusų ir kitų kenkėjiškų programų?

- Lankykitės tik su tarnybinėmis užduotimis susijusiose interneto svetainėse. Ignoruokite iššokančias reklamas, pranešimus ir kitokias žinutes.
- Nesiuntinėkite su tarnybinėmis užduotimis nesusijusių elektroninių laiškų tarnybiniu elektroniniu paštu.
- Neatidarinėkite laiškų , kurie kelia įtarimą ar gauti iš nepažįstamo siuntėjo.
- Nesisiųskite su tarnybinėmis užduotimis nesusijusių rinkmenų iš interneto.
- Darbo metu ir tarnybos reikmėms nesinaudokite viešojo elektroninio pašto sistemomis, tokiomis kaip gmail.com, yahoo.com.
- Neskelbkite su tarnyba susijusios informacijos socialiniuose ar kituose viešuosiuose tinklalapiuose.

Kaip elgtis dirbant su kompiuterinėmis laikmenomis?

! Visada patikrinkite kompiuterines laikmenas, ar jos nėra užkrėstos kenkėjiška programine įranga; duokite tai padaryti specialistams.

! Įslaptintą informaciją įkelkite tik į jau užregistruotas kompiuterines laikmenas, kurios turi būti pažymėtos tokia pat slaptumo žyma, kaip ir jose saugoma aukščiausios klasifikacijos įslaptinta informacija. Visada atkreipkite dėmesį, ar Jūsų turimos kompiuterinės laikmenos yra tinkamai pažymėtos, o baigę darbą, tinkamai jas saugokite.

! Nedirbkite ir nelaikykite tarnybinės informacijos ne darbiniuose kompiuteriuose ar laikmenose.

! Nesinešiokite kompiuterinių laikmenų iš tarnybos į namus ir atvirkščiai.

10 skaidrė: