Informacijos sauga

Kaip suvaldyti atotrūkį tarp dokumentų ir procesų

Tadas Dvarvytis

2023-03-29

ATEA

Kas yra **informacijos sauga** ir kodėl ji svarbi organizacijoms

Informacijos sauga yra **procesas**, kurio metu apsaugoma organizacijos informacija nuo neteisėtos prieigos, naudojimo, atskleidimo, modifikavimo ar sunaikinimo.

Informacijos saugos priemonėmis siekiama **užtikrinti** informacijos **konfidencialumą**, **vientisumą** ir **prieinamumą**.

Grėsmės

Statistika ir tendencijos

84%

Patyrė informacijos saugos pažeidimų

29%

Patyrė 5 ir daugiau pažeidimų

53%

Išaugo 5 kartus patyrusių pažeidimą organizacijų sk.

48%

Per 12 mėnesių kainavo daugiau nei 1 milijoną dolerių

68%

Organizacijų trūksta kibernetinės saugos kompetencijų

56%

Organizacijų nepavyksta nusamdyti darbuotojų

54%

Organizacijų nepavyksta išlaikyti darbuotojų

Debesija

Sritis kurioje rasti saugumo specialistų sunkiausiai

93%

Organizacijų vadovybių informacijos saugą prioretizuoja

83%

Organizacijų didina informacijos saugos darbuotojų skaičių

90%

Organizacijų apmokėtų sertifikavimosi išlaidas darbuotojams

Duomenys pagal *„Fortinet 2023 Cybersecurity Skills Gap Global Research Report“*

(survey of 1,855 IT and cybersecurity decision-makers)

Gerosios praktikos

Kas tarp jų bendro?

Kas aktualu **Lietuvoje**?

Lietuvos Respublikos teisės aktai

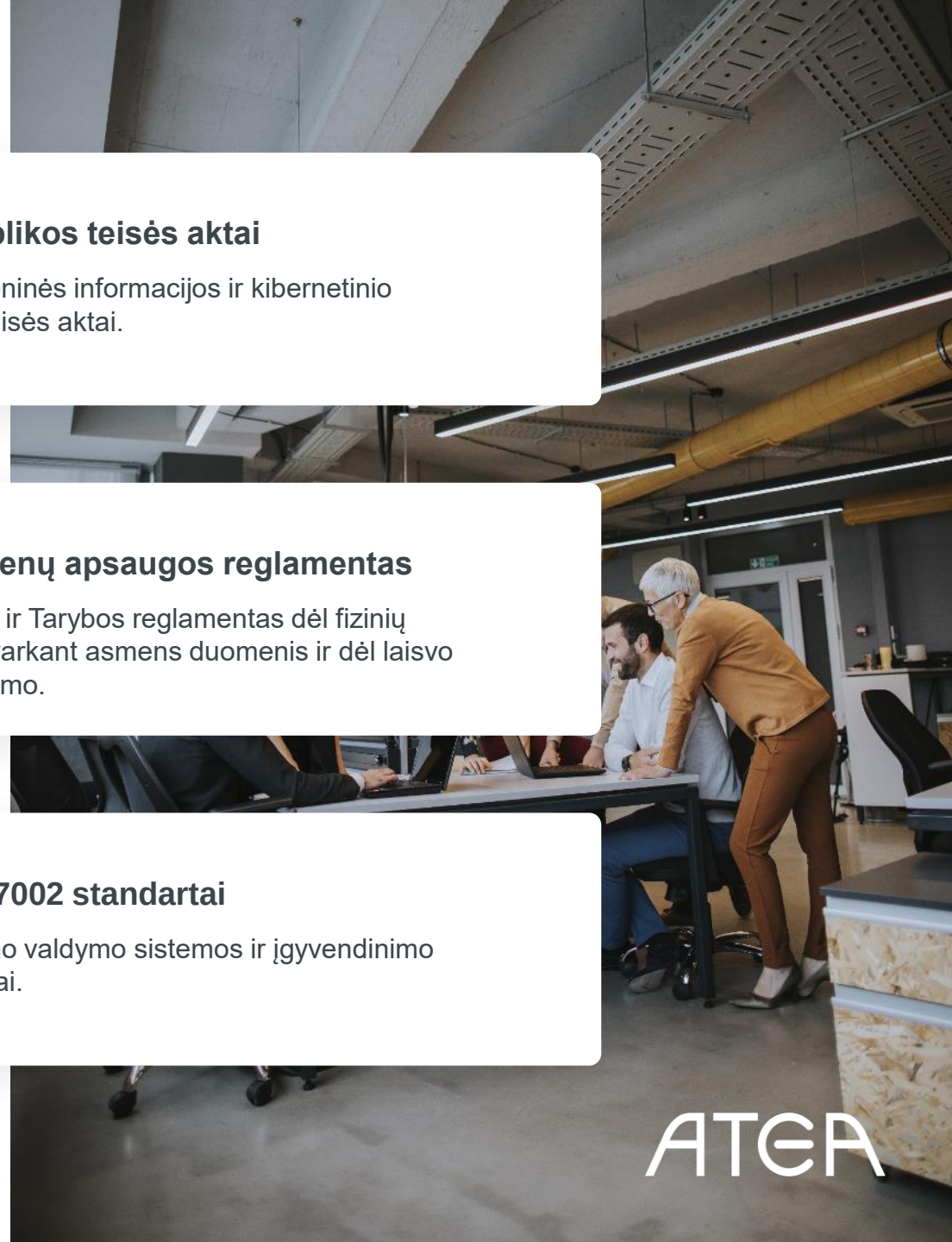
5 pagrindiniai elektroninės informacijos ir kibernetinio saugumo valdymo teisės aktai.

Bendrasis duomenų apsaugos reglamentas

Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.

ISO/IEC 27001-27002 standartai

Informacijos saugumo valdymo sistemos ir įgyvendinimo reikalavimų standartai.



Informacijos saugumo valdymo **ciklas**

Dokumentai

Svarba, valdymas

Dokumentai

Dokumentų svarba

Organizacijoms **dokumentacija** svarbi, nes ji padeda užtikrinti informacijos **saugumą**, **skaidrumą**, teisės aktų laikymąsi, **efektyvų** darbą ir nuoseklų sprendimų priėmimą bei **atsakomybės** priskyrimą.

Kokios **pasekmės** jei dokumentų nėra ar jie tvarkomi netinkamai?

Informacijos praradimas: Jei organizacijos veikla nėra tinkamai dokumentuota, gali būti prarasta svarbi informacija.

Neefektyvus darbas: Trūkstant dokumentacijos, darbuotojai gaišti laiką ieškodami reikiamos informacijos kaip atlikti tam tikras užduotis.

Atsakomybės stoka: Be dokumentacijos sunku nustatyti, atsakomybę už konkrečias veiklas ar sprendimus.

Teisinės problemos: Be dokumentų, organizacija gali patirti sunkumų įrodant savo veiklą teisiniuose ginčuose arba atitikdama teisės aktų reikalavimus.

Sunkumai naujiems darbuotojams: Nauji darbuotojai gali patirti sunkumų įsisavinant organizacijos veiklą ir kultūrą

Nustatyti reikalavimus

Pagal teisės aktus ir saugumo standartus, nustatykite, kokius reikalavimus turite įvykdyti.

Dokumentų valdymo politika

Sukurkite politiką, kuri apibrėžtų, kaip tvarkomi, saugomi, archyvuojami ir sunaikinami dokumentai.

Auditas ir stebėsena

Reguliariai tikrinkite ir stebėkite, kaip veikia jūsų dokumentų valdymo sistema.

Nuolatinis tobulinimas

Remdamiesi auditų rezultatais ir darbuotojų grįžtamuoju ryšiu, nuolat tobulinkite savo dokumentus

Technologijų naudojimas

Naudokite dokumentų valdymo sistemas (DVS) dokumentų valdymo procesams automatizuoti.

Mokymas

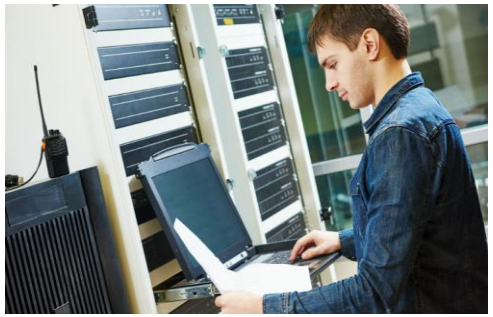
Organizuokite mokymus apie informacijos saugumo reikalavimus, įskaitant dokumentų valdymą.

ATEA

Procesai

Svarba, valdymas

Procesai



Procesų svarba

Organizacijoms svarbu nustatyti procesus, nes jie padeda užtikrinti **nuoseklų**, **efektyvų** ir **kokybišką** darbą**, sumažina klaidų** tikimybę ir **palengvina** naujų darbuotojų **įsitraukimą** bei bendradarbiavimą tarp komandų.

Kokios **pasekmės** jei procesai **nenustatyti** ar jie **vykdomi netinkamai**?

Nuostatų nesilaikymas: Be aiškių procesų, darbuotojai gali nesilaikyti nuostatų ir saugumo reikalavimų

Klaidos ir nesuderinamumas: Trūkstant nustatytų procesų, gali atsirasti nesuderinamų ar prieštaringų veiksmų.

Sunkumai atskleidžiant saugumo incidentus: Be nustatytų procesų, gali būti sunku greitai ir efektyviai atskleisti ir spręsti saugumo incidentus.

Nepakankamas darbuotojų suvokimas: Trūkstant aiškių procesų, darbuotojai gali nepakankamai suprasti informacijos saugos principus.

Nepakankama incidentų prevencija: Be nustatytų procesų, organizacija gali praleisti svarbius žingsnius, reikalingus incidentų prevencijai.

Procesų identifikavimas

Išsiaiškinkite informacijos saugumą veikiančius procesus organizacijoje ir juos stebėkite ir valdykite.

Procesų analizė

Atidžiai išanalizuokite kiekvieną procesą, identifikuokite galimus saugumo pažeidimus ir rizikos veiksnius.

Procesų optimizavimas

Optimizuokite procesus taip, kad jie būtų kuo efektyvesni ir saugesni.

Procesų stebėjimas ir kontrolė

Stebėkite ir kontroliuokite procesus, kad galėtumėte pastebėti problemas ir imtis korekcinių veiksmų.

Atsakomybės ir įgaliojimai

Nustatykite atsakomybių ir įgaliojimų lygius informacijos saugumo procesų valdymui.

Nuolatinis tobulėjimas

Vertinkite informacijos saugumo procesus reguliariai, siekdami nuolatinio tobulėjimo.

ATEA

Atotrūkis

Kodėl atsiranda atotrūkis tarp dokumentų ir procesų?
Kaip tai suvaldyti?

Atotrūkio **priežastys**

- Nepakankama komunikacija
- Neaiškūs arba sudėtingi dokumentai
- Procesų ir politikų neatnaujinimas
- Neefektyvus įgyvendinimas
- Trūksta išteklių

Rekomendacijos

Aiškiai komunikuokite

Užtikrinkite, kad informacijos saugumo politikos ir procedūros yra aiškiai ir suprantamai pateiktos visiems darbuotojams. Tai apima reguliarius susitikimus, apmokymus ir informacijos sklaidą.

Dokumentus skirstykite pagal kategorijas

Verta informacijos saugumo dokumentus skirstyti į politikas, procedūras ir techninių konfigūracijų aprašymus. Taip galėsite turėti aiškią struktūrą ir bus paprasčiau dokumentus atnaujinti, tad efektyvumas bus didesnis. Darbuotojas galės naudoti tos kategorijos dokumentą kuris reikalingas konkrečiam procesui įgyvendinti.

Periodiškai ir laiku peržiūrėkite ir atnaujinkite dokumentus

Aplinka ir procesai nuolat keičiasi, tad būtina iškart pasikeitus procesui atnaujinti ir jį aprašantį dokumentą. Neatnaujintos procedūros ar techninių konfigūracijų dokumentai incidentų atveju gali pridaryti daugiau žalos nei pats incidentas nes inžinierius kuris nebuvo proceso pakeitimo dalyvis elgsis pagal turimą dokumentą. Periodiškai peržiūrėdami dokumentus būsite tikri, kad juose informacija yra aktuali. Taip pat tai puikus laikas tobulinti procesą ir dokumentą.

Rekomendacijos

Užtikrinkite tinkamą procesų įgyvendinimą

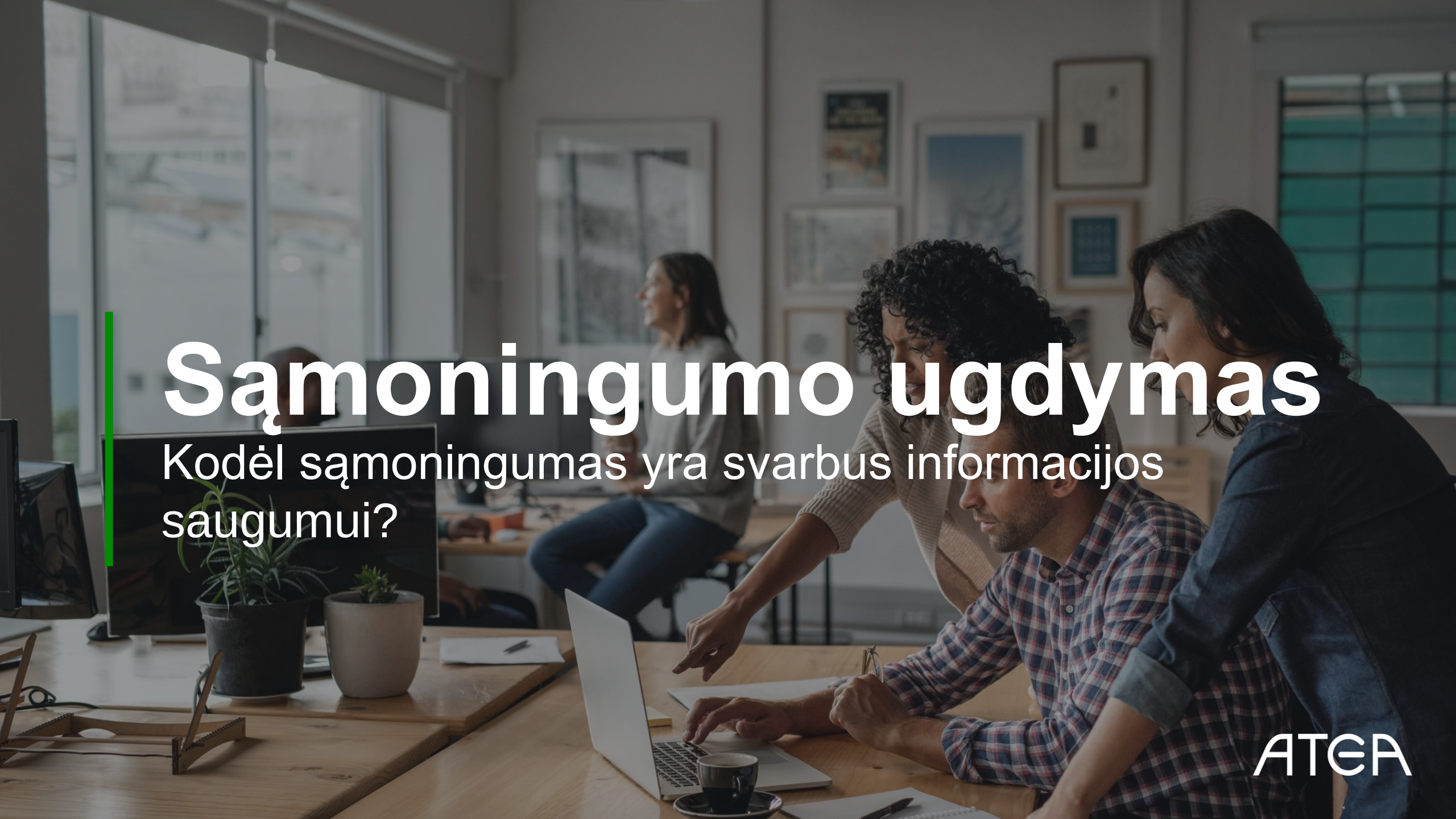
Stiprinkite informacijos saugumo procesų įgyvendinimą, taikydami nuoseklų ir sistemingą požiūrį. Tai apima prieigos kontrolės mechanizmus, reguliarią stebėseną ir kitas saugumo priemones. Nustatykite ir įgyvendinkite pasekmes darbuotojams, kurie nesilaiko informacijos saugumo reikalavimų arba nesugeba atlikti savo vaidmenų. Pasekmės gali būti įvairios, nuo įspėjimų iki darbo vietos praradimo, priklausomai nuo pažeidimo sunkumo.

Skirkite reikiamus išteklius

Skirkite pakankamai laiko, žmonių ir finansinių išteklių informacijos saugumo procesams įgyvendinti ir palaikyti. Tai apima tiek technologijų diegimą, tiek darbuotojų mokymą ir atnaujintos dokumentacijos palaikymą.

Vykdykite auditus ir kontrolė

Reguliariai tikrinkite informacijos saugumo politikų ir procesų įgyvendinimą, atlikdami vidinius ir išorinius auditus. Tai padės nustatyti galimus trūkumus ir suteiks galimybę tobulinti procesus.



Sąmoningumo ugdymas

Kodėl sąmoningumas yra svarbus informacijos saugumui?

ATEA

Kaip veikia **kibernetiniai nusikaltėliai**?

Statistika rodo, kad piktavaliai pasirenka atakas per darbuotojus tokias kaip **socialine inžinerija** paremti el. laiškai, **silpnų slaptažodžių** aptikimas ar **kenkėjiško programinio kodo** platinimas.

81%

Atakų pasinaudojant darbuotoju

19%

Kiti atakų būdai

ATEA

Kodėl verta **investuoti į** darbuotojų **sąmoningumą**

Žmogiškasis faktorius

Daugelis informacijos saugumo incidentų susiję su darbuotoju. Sąmoningi darbuotojai yra labiau atsargūs ir mažiau linkę padaryti klaidas, susijusias su informacijos saugumu.

Prevencija

Sąmoningi darbuotojai gali padėti išvengti incidentų, atpažindami potencialias grėsmes, pavyzdžiui, įtartinus el. laiškus, netinkamą prieigos kontrolę ir imdamiesi atitinkamų veiksmų juos neutralizuoti.

Atsakomybė

Sąmoningi darbuotojai supranta savo atsakomybę už informacijos saugumą ir yra pasirengę laikytis organizacijos nustatytų politikų ir procedūrų.

Tikslo atkakliai siekiantis žmogus susiranda **priemonių**, o jei negali jų rasti, **sukuria**.

- Viljamas Eleris Čeningas


We build the future with IT
ATEA.LT
ATEA.ES
ATEA
ATEA
Security