KIBERDROŠĪBA UZŅĒMUMĀ

KĀ TO IETEKMĒ VADĪBAS UN DARBINIEKU ATTIEKSME?

Andris Gailītis
Valdes priekšsēdētājs

2015. gada 1. oktobris

KAS NODROŠINA DROŠĪBU UZŅĒMUMĀ?

deac DATU CENTRI

WWW.DEAC.EU

NOTEIKUMI?

deac DATU CENTRI

WWW.DEAC.EU

CILVĒKI?

TEHNISKIE RESURSI?

deac DATU CENTRI

WWW.DEAC.EU

DROŠĪBAS NOTEIKUMI

Ja uzņēmumā ir formāli dokumentēti drošības noteikumi, vai ar to ir pietiekami?

Vai kāds seko līdzi tam vai paši noteikumi ir pietiekami pilnīgi un aktuāli?

Vai kāds seko līdzi tam vai šie noteikumi vispār tiek ievēroti?

VADĪBAS ATTIEKSME

Vadības uzskats, ka noteikumi attiecas tikai uz «parastajiem» darbiniekiem.

Uzņēmuma vadība uzskata, ja noteikumu ievērošana nepalielina uzņēmuma peļņu, tad šādi noteikumi nav vajadzīgi.

Drošība = Izdevumi

(tātad jāmēģina pēc iespējas ietaupīt).

IT SPECIĀLISTU ATTIEKSME

Paši IT speciālisti nolaidīgi attiecas pret paroļu maiņu.

77 % Izmanto vienu paroli gadu un vairāk.

21 % Izmanto vienu paroli ilgāk par 10 gadiem.

73 % Izmanto vienu un to pašu paroli vairākās vietnēs.

deac DATU CENTRI

WWW.DEAC.EU

IT SPECIĀLISTU ATTIEKSME

Paši IT speciālisti nolaidīgi attiecas pret paroļu maiņu.

Operatīvi nedzēš bijušo darbinieku kontus.

Neauditē esošajiem darbiniekiem piešķirtās pieejas un uzinstalēto programmu nepieciešamību.

«Dala visiem pa labi un pa kreisi» administratora tiesības uz darba stacijām.

LIETOTĀJU ATTIEKSME

Parastie lietotāji ne vienmēr zina (vai arī negrib zināt), ko viņi drīkst darīt ar saviem datoriem.

Nelicencētu programmu instalēšana un lietošana.

«Pirātisku» audio un video failu lejupielādēšana un glabāšana.

Nedrošu interneta vietņu apmeklēšana.

LIETOTĀJU ATTIEKSME

Ļoti bieži lietotāji savām mobilajām iekārtām pieslēdz darba e-pasta kontus – un salīdzinoši bieži lietotāja mājās šo mobilo iekārtu lieto arī citi viņa ģimenes locekļi.

Ja lietotājs nozaudē vai arī viņam tiek nozagta viņa mobilā iekārta – vai vienmēr viņš par to informē savu darba devēju?

TEHNISKIE RESURSI

Antivīrusu programmas lietošana – vai tā tiek regulāri atjaunota.

Ugunsmūris – vai ir ieviests atbilstošs tehniskais risinājums.

TEHNISKIE RESURSI

Datoru (un citu iekārtu) pārvaldības rīki – vai izvēlētais tehniskais risinājums ir drošs.

Vai visiem (būtiskajiem) datiem tiek veidotas regulāras rezerves kopijas – kāds ir izvēlētais tehniskais risinājums un vai tāds vispār ir.

(NE)ATĻAUTIE TEHNISKIE RESURSI

Ļoti izplatīta ir dažādu ārējo tehnisko resursu lietošana(gan oficiāli, gan neoficiāli), lai gan pārliecības par to lietošanas drošību NAV.

(NE)ATĻAUTIE TEHNISKIE RESURSI

Ja netiek domāts par centralizētu tehnisku risinājumu datu uzglabāšanai, darbinieki paši sāk izmantot publiski pieejamos resursus – Dropbox, Google Drive, Copy, utt.

(NE)ATĻAUTIE TEHNISKIE RESURSI

Ja uzņēmuma rīcībā nav licencētas nepieciešamās programmas, darbinieki sāk izmantot dažādas nelicencētas programmas uzņēmuma vajadzībām, lai atvieglotu savu darbu – mārketinga e-pastu izsūtīšanai, utt.

(NE)ATĻAUTIE TEHNISKIE RESURSI

Ja nav ieviests savs iekšējās komunikācijas rīks, tad darbinieki iekšējai komunikācijai un, diemžēl, arī failu apmaiņai sāk izmantot citus pieejamos rīkus – Skype, Facebook, WhatsApp, utt.

Absolūti drošs ir tikai tas dators, kas nav pieslēgts internetam un kuram tehniski nav iespējams pievienot ārējās iekārtas.

SAPRĀTĪGA DROŠĪBA

Sabalansētas biznesa un drošības prasības – nepieciešams izvērtēt drošības riskus un izlemt ar kādiem riskiem mēs esam gatavi «sadzīvot».

Apdrošināt riskus vai arī rēķināties ar potenciāliem zaudējumiem.

PALDIES!