dots.

IT drošības speciālista pakalpojums

IT drošības speciālista pakalpojums.

Pieredzējušu, augsti kvalificētu drošības speciālistu pakalpojumi uzņēmumiem, kuriem (dažādu apstākļu dēļ) drošības speciālists ir nepieciešams īslaicīgi vai tikai specifiskiem, konkrētiem mērķiem, tādējādi samazinot IT izdevumus.

Kam tas ir nepieciešams?

Uzņēmumiem, darbojoties dinamiskā, strauji mainīgā biznesa vidē, regulāri rodas situācijas, kurās drošības speciālista pakalpojumi ir nepieciešami īslaicīgi, lai palīdzētu atrisināt konkrētus izaicinājumus. Vai arī uzņēmumiem, kuriem vienmēr mainīgajos apstākļos ir nepieciešams nodrošināt pilnvērtīgu un ilgtermiņa IT drošību, tajā pašā laikā nepalielinot vai pat samazinot IT drošības izdevumus.

Kā šis pakalpojums strādā?

Lai palīdzētu uzņēmumiem risināt situācijas, kurās nav ekonomiskā pamatojuma algot pastāvīgu drošības speciālistu, uzņēmums dots. piedāvā visaptverošu palīdzību, ļaujot efektīvi pārvaldīt drošības riskus. Izvēloties šo pakalpojumu, Jūsu uzņēmumam tiks piesaistīta IT drošības komanda, no kuras noteiktam uzdevumam tiks izvirzīts atbilstošākais drošības speciālists, lai veiktu nepieciešamo IT drošības uzdevumu Jums vajadzīgajā apjomā.

IT drošības speciālista pienākumos ietilps:

IT dokumentācijas sagatavošana un atbilstības nodrošināšana;

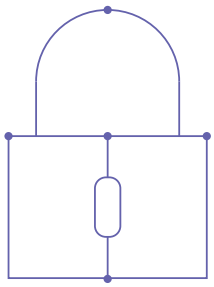
Regulāra IT risku identificēšana un riska līmeņa uzraudzība;

Lietotāju apmācība;

SIEM, IPS, DLP sistēmu ieviešana un uzraudzība;

IT sistēmu ievainojamību pārbaude un drošības testu veikšana;

Uzņēmuma vadības, administratoru un programmatūras izstrādes komandas konsultēšana.



dots.

Kas ietilpst pakalpojumā?

Tehniskās konsultācijas:

Atbildes saistībā ar IT drošības jautājumiem;
Informācijas sistēmu drošas konfigurācijas izveide;
Trešo pušu drošības risinājumu pārvaldības jautājumi;
Jaunu IS izstrādes vai nozīmīgu izmaiņu gadījumā.

IT drošības incidentu izmeklēšana

Nepieciešamās IT drošības dokumentācijas sagatavošana un regulāra atjaunošana
(politikas, procedūras un instrukcijas)

Publiski pieejamo resursu ievainojamību skenēšana
(reizi mēnesī)

Iekštīkla ievainojamību skenēšana
(reizi ceturksnī)

Izmantoto tehnoloģisko rīku konfigurācijas izvērtēšana

IT drošības risku pārvaldība:

Risku analīzes sagatavošana;
Risku reģistra uzturēšana un aktualizēšana;
Ieviešamo kontroļu atsekošana.

IT drošības risku mazinošo pasākumu koordinēšana un rezultātu atsekošana
(piemēram, drošības atjauninājumu uzstādīšana, programmatūras konfigurācijas un programmu koda izmaiņas).

Lietotāju pieejas tiesību audits
(reizi ceturksnī)

Lietotāju apmācības, izpratnes veicināšanas pasākumi, sociālās inženierijas tests
(pēc nepieciešamības)

IT sistēmas darbības un konfigurācijas atbilstības pārbaudes iekšējiem IT drošības standartiem

IT drošības situācijas ziņojuma sagatavošana vadībai

Atbalsts ārējos sertifikācijas auditos
(piemēram, ISO 27001, 9001)

dots.

Ieguvumi

Atbrīvo
no maznozīmīgiem rutīnas darbiem, lai varat pievērsties uzņēmuma pamatdarbības prioritātēm. Tie ir tādi darbi, kas ir viegli nododami citiem, piemēram, jauno ievainojamību klasifikācija, lietotāju inventarizācija.

Rada
piekļuvi nepieciešamai papildus kompetencei, piemēram, regulāra konfigurācijas caurskatīšana. Ļoti svarīgi, jo vienā uzņēmumā ir daudz tehnoloģisku iekārtu un viens drošības specialists nevar būt vienlīdz kompetents visās.

Finanšu caurskatāmība
Uzņēmuma vadītājam ir skaidri redzamas veicamo darbu izmaksas, un tās var attiecināt uz konkrētiem projektiem (kapitalizēt).

Mērogojamība
strauji attīstot jaunu produktu, uzņēmumam rodas nepieciešamība piesaistīt papildus resursus uz neilgu laiku, piemēram, 3-6 mēneši.

Individualizēti
un izdevīgi drošības pakalpojumi atkarībā no uzņēmuma vajadzībām.

Nodrošinām
neatkarīgu izvērtējumu, kas izslēdz darbinieku savstarpējo ieinteresētību piesegt kolēģus.

WeAreDots, SIA
Elizabetes iela 75, Rīga
Latvija LV-1050

+371 67509912
info@wearedots.com