KPMG

Cik kiberdrošas ir Latvijas pašvaldības?

KPMG Baltics SIA

2019. gads

Saturs

Ievads

Mūsdienu tehnoloģiju laikmetā gan privātajā, gan publiskajā sektorā arvien vairāk tradicionālo procesu un pakalpojumu tiek uzticēti informācijas un komunikāciju tehnoloģijām. Tās palīdz iegūt un apstrādāt informāciju, izmantot savstarpējās saziņas rīkus un platformas un saņemt pakalpojumus. Taču vienlaikus līdzās virknei priekšrocību, ko sniedz mūsdienu tehnoloģijas, ir radušies jauni drošības riski, tajā skaitā interneta vietnēm.

Lai novērtētu Latvijas pašvaldību mājaslapu kiberdrošību, tajās esošo datu noplūdes iespējamo apdraudējumu un izstrādātu atbilstošas rekomendācijas kiberrisku mazināšanai, KPMG sadarbībā ar Latvijas Pašvaldību savienību (LPS) un Vides aizsardzības un reģionālās attīstības ministriju (VARAM) īstenoja projektu "Cik kiberdrošas ir Latvijas pašvaldības?". Tā ietvaros KPMG veica kiberdrošības pārbaudes 15 dažādu lielumu Latvijas pašvaldību mājaslapām, kā arī novērtēja kiberhigiēnas jeb pašvaldības darbinieku izpratnes līmeni par kiberdrošību.

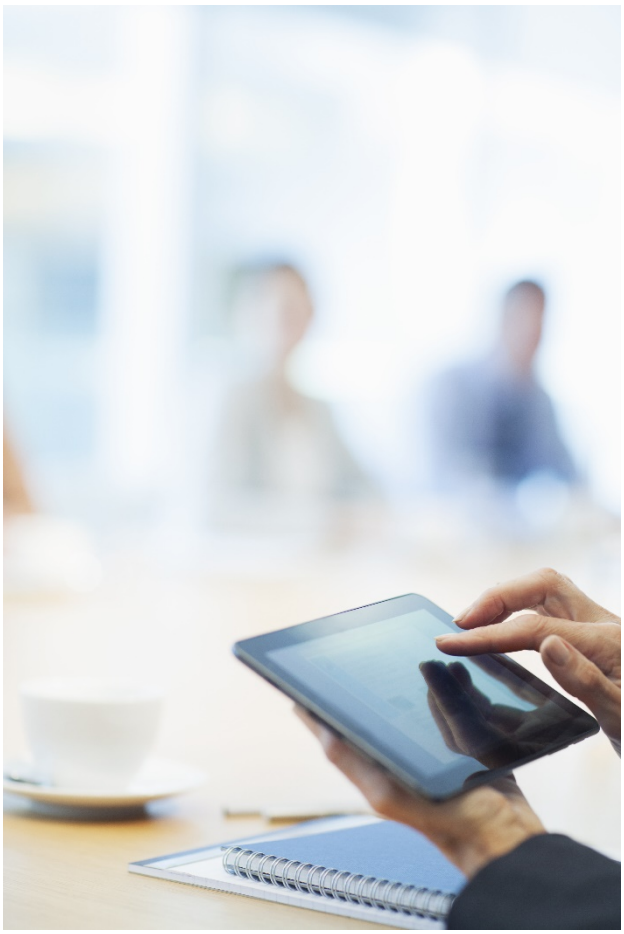
Projekta noslēgumā katra no iesaistītajām pašvaldībām saņēma apkopotu informāciju par identificētajām ievainojamībām, kā arī individuālus ieteikumus nepieciešamajiem uzlabojumiem.

Šajā materiālā apkopotā veidā ir sniegti projekta rezultāti, kas ļauj apzināt kopējo situāciju kiberdrošības jomā Latvijas pašvaldībās – darbinieku kibervieduma līmeni un interneta vietņu drošības līmeni - arī tām pašvaldībām, kas projektā nepiedalījās.

Projekta apraksts

Novērtējums tika veikts 15 dažādu lielumu Latvijas pašvaldībās. Ņemot vērā iedzīvotāju skaitu pašvaldībās, tās tika iedalītas trīs grupās: lielās pašvaldības – virs desmit tūkstošiem iedzīvotāju, vidēja lieluma pašvaldības – no četriem līdz desmit tūkstošiem iedzīvotāju un mazās pašvaldības ar iedzīvotāju skaitu zem četriem tūkstošiem. Šāds iedalījums ļāva pārbaudīt, vai pastāv likumsakarība starp pašvaldības lielumu, attiecīgi arī tās resursiem un finansiālajām iespējām, un pašvaldības rādītājiem kibedrošības jomā.

Arvien vairāk pakalpojumu ikdienā saņemam attālināti: sniedzam pieteikumus valsts iestādēm, apmaksājam rēķinus, piesakāmies konsultācijām. Izmantot digitālās vides priekšrocības ir ātri un ērti. Bet cik droši? Viens no pētījuma mērķiem bija noskaidrot, cik drošas ir Latvijas pašvaldību mājaslapas, tādējādi secinot, vai pašvaldības ir gatavas digitālo pakalpojumu ērai.



Tīmekļa vietņu drošības novērtēšana tika veikta, izmantojot starptautiski atzītās OWASP drošības testēšanas vadlīnijas. Tīmekļa vietnes kiberdrošības novērtēšanā KPMG izmantoja gan manuālas, gan automatizētas metodes, kā arī standarta automatizētos testēšanas rīkus. Projekta ietvaros tika pielietota metode, kas simulē ārēja uzbrucēja uzvedību. Tādā veidā bija iespējams noskaidrot, ar kādiem drošības kontroļu apiešanas līdzekļiem iespējams iekarot pašvaldību mājaslapas.

OWASP (Open Web Application Security Project) ir pasaules mēroga bezpeļņas organizācija, kuras darbības mērķis ir vērsts uz programmatūras drošības uzlabošanu.

Drošības kontroles ir aizsargpasākumi, kurus izmanto, lai novērstu, atklātu, atvairītu vai samazinātu drošības riskus fiziskajam īpašumam, informācijai, datoru sistēmām vai citiem aktīviem.

Informācija novērtējuma veikšanai tika iegūta tikai no pašvaldības tīmekļa vietnes. Novērtējuma veikšanas procesā pašvaldību mājaslapās tika atrastas vairākas ievainojamības. Katram atklājumam tika noteikta riska pakāpe un sniegti ieteikumi, kā mazināt šo risku.

Ielaušanās testi ir kāda informācijas resursa uzlaušanas mēģinājums. Testi tiek veikti, lai izprastu resursa drošības līmeni un atrastu ievainojamības un resursa ievainojamās vietas. Svarīgi, ka ielaušanās testēšana ļauj izprast izmantoto aizsardzības līdzekļu efektivitāti.

Mājaslapu kiberdrošības pārbaudes rezultāti

Pašvaldību mājaslapās atklātās ievainojamības tika iedalītas trīs riska grupās: augsts riska līmenis, vidējs riska līmenis un zems riska līmenis. Jāpiebilst, ka vairākas zema riska līmeņa neatbilstības vienkopus var veidot augsta līmeņa risku pašvaldību tīmekļa vietnēm.

Riska līmeņa klasifikācija

Augsts riska līmenis

Norāda uz paaugstinātas hakeru, vīrusu vai citu ļaunprātīgu darbību risku. Pastāv augsta iespējamība, ka var notikt datu noplūde vai mājaslapa var tikt pilnībā pārņemta reāla uzbrukuma laikā.

Vidējs riska līmenis

Norāda uz būtisku hakeru, vīrusu vai citu ļaunprātīgu darbību risku. Veiksmīga uzbrukuma laikā ir iespējams ievainot mājaslapu, izraisīt traucējumus mājaslapas darbībā vai pārņemt lietotāju datus.

Zems riska līmenis

Norāda, ka hakeru, vīrusu vai citu ļaunprātīgu darbību risks ir iespējams. Mājaslapas ievainojamās vietas potenciāli var tikt izmantotas kibernoziegumu veikšanai.

Pēc novērtējuma rezultātiem katrā pašvaldības tīmekļa vietnē tika identificētas ievainojamības, kas var būtiski ietekmēt tīmekļa vietnes drošību.

Augsta riska līmeņa ievainojamības tika atklātas 10 no 15 novērtētajām pašvaldību tīmekļu vietnēm

10 no 15

pašvaldībās tika atklātas augsta riska līmeņa ievainojamības

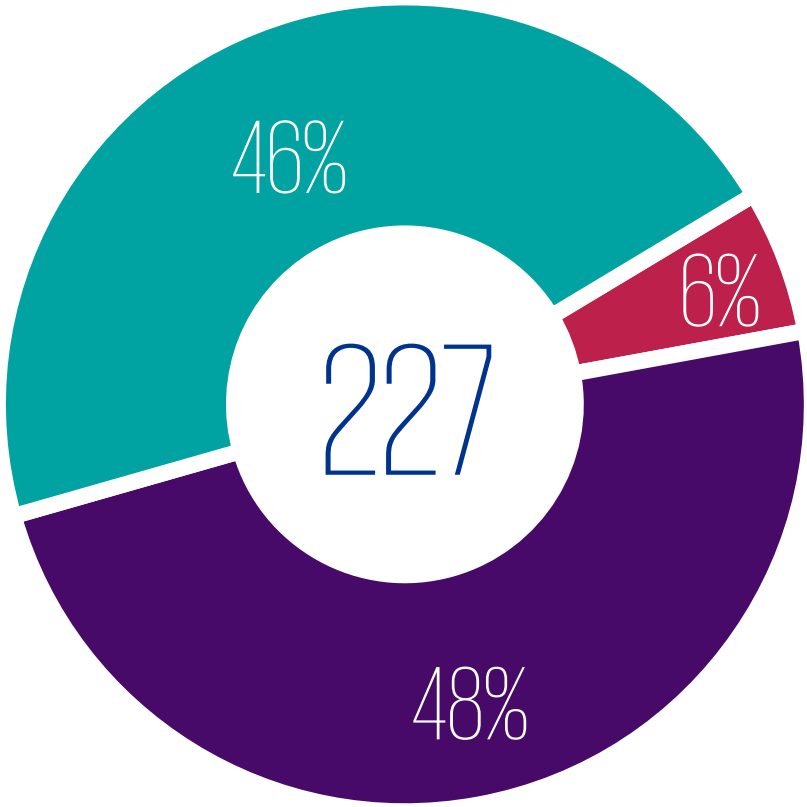
Visās

pašvaldībās tika atklātas vidējā riska līmeņa ievainojamības

Visās

pašvaldībās tika atklātas zema riska līmeņa ievainojamības

Atklāto ievainojamību sadalījums pēc riska līmeņiem



Novērtējuma laikā, veicot pārbaudes un mēģinot piekļūt organizācijas IT sistēmu iekšējai informācijai, visās 15 pašvaldībās kopā tika atklātas 227 ievainojamības

Dažās pašvaldībās tika konstatētas 4-5 ievainojamības, tomēr bija pašvaldības, kur atklāto ievainojamību apjoms sasniedza 20 un vairāk. No kopējā ievainojamību skaita 6% veidoja augsta riska ievainojamības. Šī riska līmeņa ievainojamības ir būtiski novērst nekavējoties, jo ir liela iespējamība, ka reāls uzbrucējs spēs pārņemt kontroli pār mājaslapu vai padarīt resursu nepieejamu, tādā veidā radot gan kaitējumu reputācijai, gan finanšu zaudējumus. Vidēja riska līmeņa ievainojamības, kuru apjoms veidoja 46%, var būtiski ietekmēt organizācijas reputāciju un darbību, ja tās netiks novērstas. Zema riska līmeņa ievainojamības veidoja 48%. Arī šajā gadījumā pašvaldībām ir jādomā par mājaslapas drošības uzlabošanu, jo vairāku zema līmeņa ievainojamību vienlaicīga pastāvēšana var radīt jau nopietnāku vietnes drošības apdraudējumu.

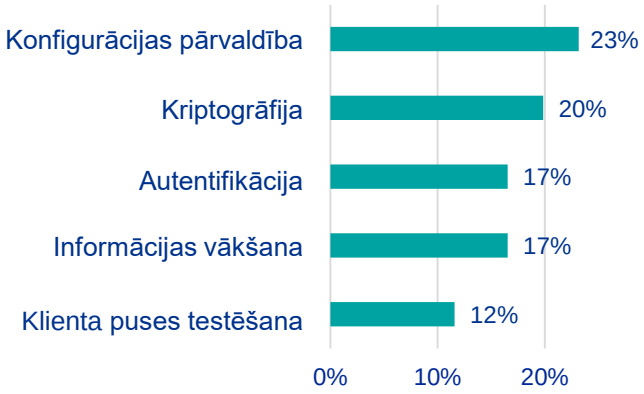
Atklāto ievainojamību jomas

Apkopojot rezultātus, tika atklātas problemātiskās jomas, kas ir raksturīgas vairākām pašvaldību tīmekļa vietnēm. Ir jāapzinās, ka drošības aspekti ir atkarīgi ne tikai no platformas, uz kuras bāzes ir uzbūvēta mājaslapa, bet arī no izmantotās versijas, iestatījumiem un, protams, informācijas tehnoloģiju speciālistiem, kas pārvalda šo sistēmu. Lielākais vājo vietu skaits tika identificēts konfigurācijas jeb mājaslapas sastāvdaļu kopuma un savstarpējo sakaru pārvaldības jomā. Šī problēma tika konstatēta vairumā pašvaldību mājaslapu.

Pārbaužu laikā tika atklāts, ka pietiktu pat ar viena datora jaudu, kas šajā gadījumā tika izmantots kiberpārbaudes veikšanai, lai pārsniegtu mājaslapas apstrādājamo pieteikumu skaitu. Tas nozīmē, ka pieprasījumi no reāliem lietotājiem šajā laikā netiktu apstrādāti. Tādā veidā uzbrucējs varētu padarīt pašvaldības resursus nepieejamus vai liktu lietotājam stundām ilgi gaidīt atbildi no sistēmas. Lai mazinātu šāda riska ietekmi, ir būtiski sekot visiem pieejamiem atjauninājumiem, lai pasargātu savu tīmekļa vietni no iespējamiem kiberuzbrukumiem un ieviestu proaktīvus drošības risinājumus.

Vislielākais vājo vietu skaits tika identificēts konfigurācijas jeb mājaslapas sastāvdaļu kopuma un savstarpējo sakaru pārvaldības jomā

Kādās jomās tika atrasts vislielākais ievainojamību skaits?



Konfigurācijas pārvaldība

Konfigurācijas vadība apskata produkta attīstības funkcionālo un fizisko komponentu pārvaldību. Ja organizācijas mājaslapai rodas problēmas ar konfigurācijas pārvaldību, kiberuzbrucējs var viegli padarīt mājaslapu nepieejamu, patvaļīgi mainīt mājaslapas saturu un pilnībā pārņemt organizācijas mājaslapas pārvaldīšanu.

Kriptogrāfija

Kriptogrāfija ir informācijas kodēšanas nozare, kurā izstrādā informācijas šifrēšanas metodes, lai aizsargātu pret nevēlamu informācijas nolasīšanu. Ja neievēro korektas šifrēšanas nosacījumus vai šifrēšanu neizmanto vispār, datu noplūdes gadījumā visa uzglabātā informācija, piemēram, lietotāju personas dati vai organizācijas iekšējie dokumenti kļūs pieejami uzbrucējam. Piemēram, ja pašvaldības mājaslapā ievadāt savu personas informāciju, vārdu, uzvārdu, telefona numuru vai adresi, datu noplūdes gadījumā šī informācija būs lasāma uzbrucējam, kas tālāk jau var tik izmantota ļaunprātīgos nolūkos.

Autentifikācija

Autentifikācija ir process, kura laikā veic lietotāja identitātes pārbaudi datorsistēmā. Tā tiek veikta kā nākamais solis pēc identifikācijas - lietotāju atšķiršanas viena no otra. Neievērojot labo praksi autentifikācijas pārvaldībā, mājaslapas uzturētājs riskē ar lietotāju datu drošību. Uzbrucējs var izmantot ievainojamības, lai pieslēgtos lietotājiem ar dažādām pieejas tiesībām, zagtu datus, mainītu informāciju un potenciāli pārņemtu mājaslapas pārvaldību.

Informācijas vākšana

Informācijas vākšana ir pirmais drošības novērtējuma posms, kura mērķis ir iegūt pēc iespējas vairāk informācijas par mērķa mājaslapu un iespējamām ievainojamām vietām. Uzbrucējs veic informācijas vākšanu, izmantojot robotus un, ja šie roboti ir atklājuši pietiekami daudz informācijas par interneta vietni, uzbrucējs var sākt mērķtiecīgu kiberuzbrukumu.

Klienta puses testēšana

Klienta puses testēšana ir speciāls termins, kas tiek izmantots, lai pārbaudītu, vai mājaslapā var ievietot kaitīgu programmas daļu, trešās puses izstrādātu kodu, lai nodarītu kādu kaitējumu. Tādas darbības tiek veiktas, piemēram, lai nozagtu lietotāju datus brīdī, kad lietotājs tos ievada mājaslapas logos. Ļaunprātīgo kodu bieži izmanto, lai veiktu satura izmaiņas organizācijas tīmekļa vietnē, izvietotu politiskus vai radikālus materiālus. Šādā veidā uzbrucējs var dezinformēt pašvaldības iedzīvotājus, radot priekšstatu, ka informāciju izvietojusi pati organizācija. Vēl vairāk – pieprasīt izpaust personas datus vai pat piespiest pārsūtīt naudas līdzekļus uz krāpnieka kontu.

Lai maksimāli mazinātu kiberriskus pašvaldībās, tām jāveic efektīva IT resursu pārvaldība, jāseko līdzi atjauninājumiem, jāpielieto labās prakses principi kiberdrošības jomā, kā arī jāveic regulāras kiberdrošības pārbaudes.

Pašvaldību tīmekļa vietņu drošības līmeņa uzlabošana var kļūt par vienu no svarīgākajiem soļiem drošākas Latvijas kibertelpas attīstībā

Nav pilnīgi drošu sistēmu, ir sistēmas, kuras var efektīvi novērst risku un sniedz iespēju atvairīt uzbrukumu.

Pētījuma rezultāti norāda uz to, ka pētījumā ietvertās Latvijas pašvaldības nav pietiekami drošas. Pastāv liela varbūtība, ka kiberuzbrukuma laikā pašvaldību tīmekļa vietnes var tikt būtiski ievainotas. **Grūti novērtēt, kādas sekas var izraisīt veiksmīgs kiberuzbrukums katrai no pašvaldībām, jo mājaslapu funkcionalitāte atšķiras. Tomēr viennozīmīgi var teikt, ka**

veiksmīga kiberuzbrukuma gadījumā tiktu ietekmēta gan organizācijas reputācija, gan varētu rasties tieši vai netieši finanšu zaudējumi.

Kiberdrošība ir termins, ko izmanto, lai aprakstītu procesu kopu, kas vērsts uz IT aizsardzību no ļaunprātīgiem uzbrukumiem. To sauc arī par informācijas tehnoloģiju drošību vai elektronisko informācijas drošību.

Kibertelpa ir interaktīva vide, kura ietver lietotājus, tīklus, programmatūru, procesus, informācijas kopumu, pakalpojumus, lietojumprogrammas un sistēmas, kas ir savienotas, izmantojot internetu, telesakarus vai datortīklus, un kurā mijiedarbojas tās lietotāji.

IT Infrastruktūra ir aparatūra, programmatūra, tīkla resursi un pakalpojumi, kas nepieciešami organizācijas IT vides pastāvēšanai, darbībai un pārvaldībai.

Projekta noslēgumā pēc 15 Latvijas pašvaldību mājaslapu izpētes – kibernovērtējuma – veikšanas KPMG sniedza kiberdrošības ieteikumus, kurus ieviešot pašvaldībām ir iespēja būtiski uzlabot tīmekļa vietnes kiberdrošības līmeni, kā arī veicināt sistēmu ātrdarbību. Tādejādi pašvaldības jau tuvākajā laikā varētu sākt izmantot savas mājaslapas kā efektīvu digitālo rīku saziņai ar pašvaldības iedzīvotājiem. Ieteikumi balstās uz pētījuma laikā gūtajiem novērojumiem.

”

Svarīgi apzināties, ka drošībai, īpaši digitālajā vidē, nav mērķa vai galapunkta, kas ir jāsasniedz. Tas ir process, kuram vienmēr ir jāseko līdzi un jādomā soli uz priekšu, lai mazinātu iespējamā uzbrukuma sekas. Domāt par drošību nekad nav par vēlu.

“

TOP 5

ieteikumi pašvaldību mājaslapu drošības uzlabošanai

- Izmantot datu pārraides šifrēšanas risinājumus.
- Regulāri pārskatīt piekļuves pārvaldības kontroles.
- Veikt IT infrastruktūras iestatījumu pārskatīšanu saskaņā ar labo praksi.
- Izmantot drošības risinājumus netipisku darbību identificēšanai un pārvaldībai.
- Veikt regulārus kiberdrošības novērtējumus saskaņā ar starptautiskajiem standartiem.

Kaspars Iesalnieks
KPMG IT konsultāciju vadītājs

Sociālās inženierijas simulācijas rezultāti

Viens no būtiskākajiem kiberdrošības aspektiem ir cilvēku izglītotība un izpratne kiberhigiēnas jautājumos, tāpēc projekta ietvaros tika veikta sociālās inženierijas uzbrukumu simulācija 162 darbiniekiem 15 dažādās Latvijas pašvaldībās.

Pašvaldību darbiniekiem tika nosūtīts e-pasts ar kaitīgas vēstules pazīmēm, kurā tika lūgts «uzklikšķināt» uz e-pastā norādītās saites. E-pastā pašvaldības darbinieks tika uzrunāts vārdā, jo šī informācija ir brīvi pieejama potenciālam uzbrucējam pašvaldības mājaslapā. Vēstule saturēja vairākas kaitīgas vēstules pazīmes: aizdomīgu sūtītāja adresi, parakstu un citas komponentes. Saturs tika izveidots tādā veidā, lai darbinieks nepievērstu uzmanību vēstules detaļām un nospiestu uz pavienoto saiti. Uzbrucējam ir svarīgi likt lietotājam rīkoties, apiet organizācijas procedūras un instrukcijas vai ieinteresēt lietotāju ar saistošu piedāvājumu.

> 16% darbinieku, kas piedalījās simulācijā, nepamanīja kaitīgās vēstules pazīmes un reāla uzbrukuma gadījumā būtu kļuvuši par uzbrucēja upuriem.

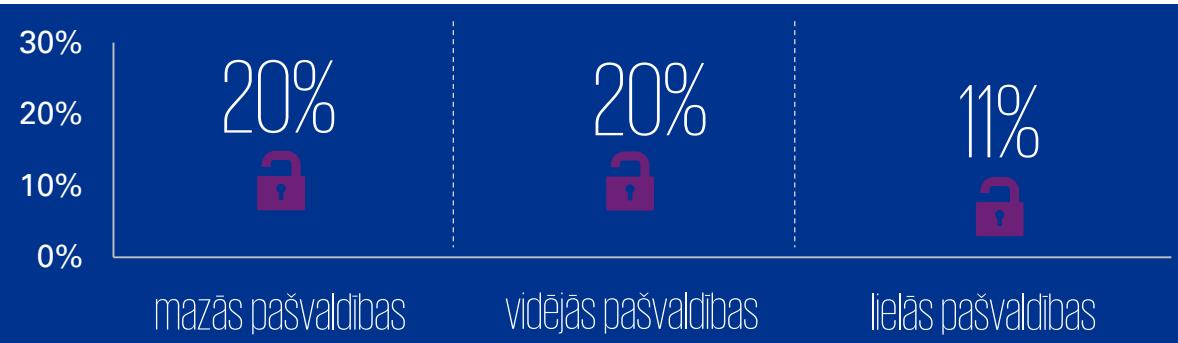
Notiekot reālam uzbrukumam, šādas saites atvēršana potenciāli varētu izraisīt neatgriezeniskas izmaiņas «upura» darba stacijā un izplatīties organizācijas tīklā. Tāpēc, redzot aizdomīgu e-pastu, nav ieteicams atvērt nosūtīto saiti, lejupielādēt pievienotos dokumentus vai spiest uz vēstules saturu.

Sociālā inženierija ir manipulācijas paņēmiens, ko pielieto, lai liktu cilvēkam rīkoties tā, kā to vēlas uzbrucējs. Uzbrucēja mērķis ir iegūt personas datus vai piekļuvi uzņēmuma resursiem vai sistēmām. Pēc «Oracle and KPMG Cloud threat report» datiem pēdējo 2 gadu laikā 55% uzņēmumu padzīvojuši pikšķerēšanas uzbrukumu.

Kiberhigiēna jeb **virtuālā higiēna** ir pasākumu kopums, ko datoru un citu ierīču lietotāji veic, lai uzturētu sistēmas veselību un uzlabotu tiešsaistes drošību. Piemēram, izmanto dažādas paroles tiešsaistes resursiem un nevienam tās nenodot.

Pikšķerēšanas uzbrukums ir īpašs interneta krāpniecības paveids, kurā, izmantojot e-pastu vai ziņu apmaiņas programmas, tiek mēģināts apmuļķot lietotāju un lietotājs tiek mudināts veikt darbības, kas var tam kaitēt. Piemēram, uzbrucējs mudina atvērt kādu saiti, atvērt inficētu e-pasta pielikumu vai atklāt savas paroles.

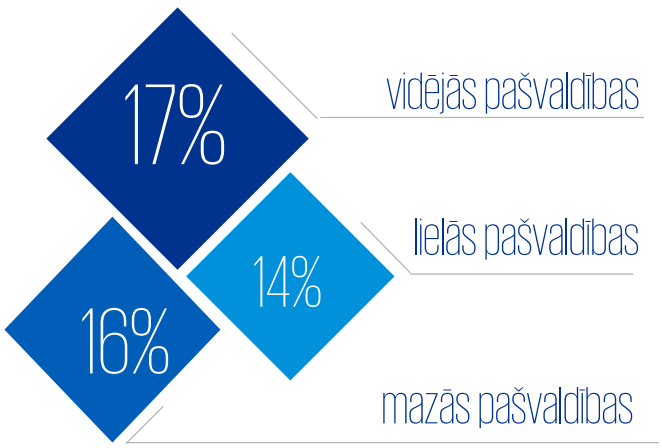
Cik procentu pašvaldību darbinieku ir atvēruši e-pastam pievienoto saiti?



Mediāna ir vidējās vērtības rādītājs un norādīta katrai pašvaldību grupai.

Neatklāto kaitīgo vēstuļu skaits

Vidējā vērtība katrai no pašvaldību grupām



Nevar viennozīmīgi apgalvot, ka kāda no pašvaldību grupām ir parādījusi labākus rezultātus salīdzinājumā ar pārējām. Kiberdošības jomā katram ir jāapzinās, kādi riski pastāv un kādas sekas tie var izraisīt. Pat viena vēstule var izraisīt neatgriezeniskas sekas. Piemēram, lielo pašvaldību grupā neidentificēto vēstuļu procents ir vidēji 14%, taču šajā grupā bija arī visaugstākais neidentificēto kaitīgo vēstuļu rezultāts – 33% vienā pašvaldībā.

Simulācijas laikā 12% no pašvaldību darbiniekiem, kas piedalījās pētījumā, ir uzklikšķinājuši uz pievienotās saites.

Savukārt 4% darbinieku, kas piedalījušies simulācijā, ir atbildējuši sūtītājam ar mērķi precizēt saites adresi. Tas varētu notikt lietotāja neuzmanības dēļ vai tāpēc, ka informācijas sistēmas aizsardzības tehniskais risinājums neļāva piekļūt šai saitei.

Uzsākot komunikāciju ar uzbrucēju, cilvēks apiet tehniskus aizsarglīdzekļus, kas ir definēti sistēmā, un var kļūt par uzbrucēja upuri.

Piemēram, uzbrucējs var sazināties ar upuri telefoniski ar mērķi precizēt informāciju, tādā veidā iegūstot informāciju ne tikai par lietotāju, bet arī par organizāciju, kurā lietotājs strādā.

12% darbinieku

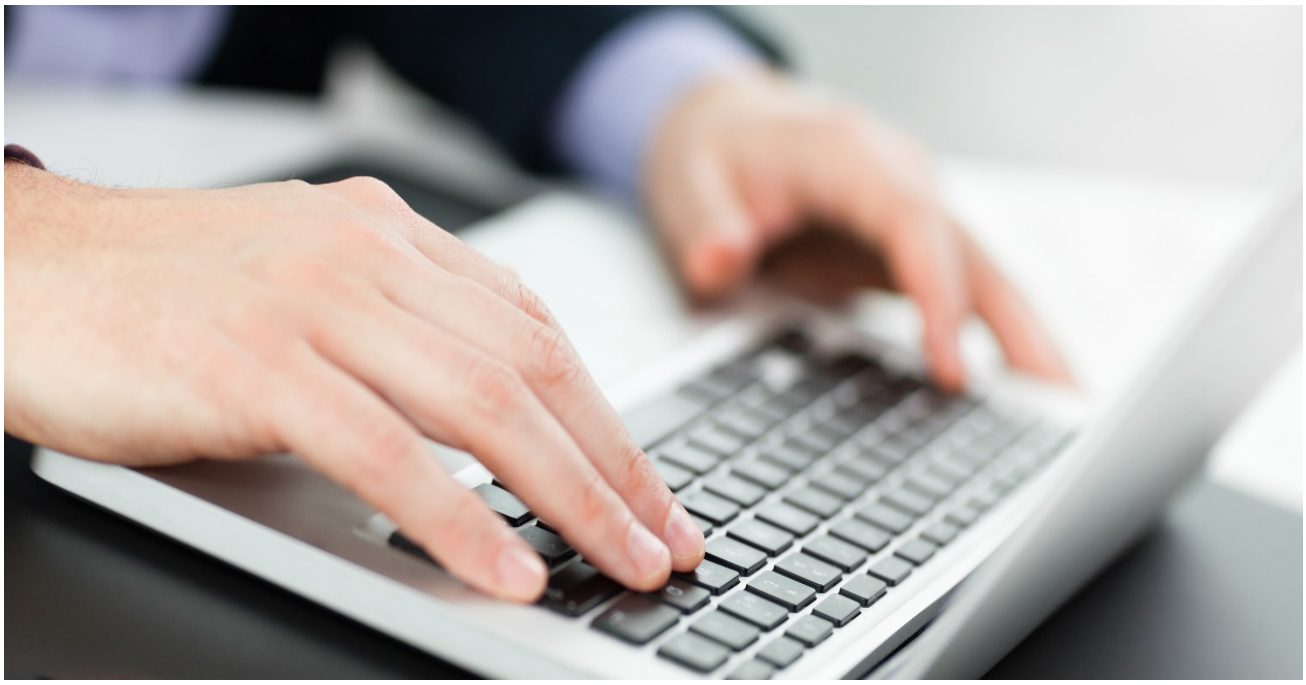
Ir uzklikšķinājuši uz e-pastam pievienotās saites

4% darbinieku

Ir sākuši komunikāciju ar aizdomīgās vēstules sūtītāju

2 pašvaldības

Netika identificēts, ka darbinieki ir pārgājuši uz pievienoto saiti.



TOP 5

kaitīgo vēstuļu pazīmes

- E-pasta sūtītāja vārds un uzvārds nesakrīt ar e-pasta adresi, no kuras e-pasts ir nosūtīts.
- E-pasts parakstīts ar vispārīgu sūtītāja apzīmējumu.
- E-pasti no uzņēmumiem vai organizācijām, ar kuriem saņēmējām nav nekāda sakara.
- E-pasti, kuros ir iekļautas saites, virs kurām turot kursoru, parādās citāda saites adrese nekā e-pasta tekstā.
- Piedāvājumi, kas ir pārāk labi, lai būtu patiesi.

Divās pašvaldībās, kas piedalījās simulācijā, darbinieki nav atvēruši e-pastam pievienoto saiti. Tāds rezultāts, iespējams, varēja tikt sasniegts, pateicoties sistēmā definētajiem tehniskajiem aizsarglīdzekļiem.

Jāatzīmē, ka dažu pašvaldību darbinieki ir ziņojuši par aizdomīgiem e-pastiem organizācijas atbildīgam personālam. Tas ir labākais veids, kā rīkoties, ja ir saņemta aizdomīga vēstule.

Rezultāti rāda, ka kopumā pašvaldību darbiniekiem nav pietiekoši attīstīts kiberhigiēnas līmenis, un tā diemžēl ir izplatīta situācija, kas var novest pie nevēlamām sekām.

Tomēr zināšanas par kiberhigiēnu un prasmes tās ievērošanā ir viegli attīstīt, regulāri organizējot praktiskas apmācības un sociālās inženierijas simulācijas, kas palīdz sagatavot organizācijas darbiniekus reālam uzbrukumam. Būtiski ir iedrošināt darbiniekus ziņot par aizdomīgām vēstulēm un pārliecināties, vai katrs no darbiniekiem zina, kā notiek incidentu ziņošanas process. Ir jāatceras, ka dažreiz pat viena pāreja uz kaitīgo saiti var inficēt ne tikai viena darbinieka darbstaciju, bet izplatīties visā organizācijas tīklā.

Kaspars Iesalnieks
KPMG IT konsultāciju vadītājs

KPMG Baltics SIA
Vesetas iela 7
Rīga, LV-1013

T: 67038000
E: kiesalnieks@kpmg.com

kpmg.com/socialmedia