Ikmēneša informācijas drošības izdevums tev

# Ikviens var uzsākt karjeru kiberdrošības jomā

## Pārskats

Par kiberdrošību mēs lasām ziņās gandrīz katru dienu, jo organizācijas un valdības visā pasaulē cieš no izspiedējvīrusiem, krāpniecības un kiberuzbrukumiem. Ir milzīgs pieprasījums pēc speciālistiem, kuri ir apmācīti kiberdrošības jomā, lai palīdzētu aizsargāties pret šiem pieaugošajiem draudiem. Faktiski jaunākie pētījumi liecina, ka pasaulē ir gandrīz 3 miljoni darba vietu kiberdrošības jomā.

Vai esat domājis par kiberdrošības profesionāļa karjeru? Tā ir strauja, ļoti dinamiska joma ar lielu skaitu aizraujošu specialitāšu, no kurām izvēlēties. Šīs ir pozīcijas tādās jomās kā kriminālistika, izpratne un apmācība, galapunktu aizsardzība, kritiskā infrastruktūra, reaģēšana uz incidentiem, droša kodēšana un politika. Karjera kiberdrošības jomā arī ļauj strādāt gandrīz jebkur pasaulē, tā nodrošina dažādas priekšrocības un iespēju panākt reālas pārmaiņas.

## Vai man ir nepieciešams grāds datorzinātnēs?

Pilnīgi noteikti, nē. Daudziem no labākajiem drošības speciālistiem ir iepriekšējā pieredze jomās, kas nav saistītas ar tehnoloģijām. Galvenais ir aizrautīga mācīšanās; tiklīdz jūs saprotat, kā tehnoloģijas darbojas (un var tikt uzlauztas), jūs varat tās labāk pasargāt. Kiberdrošība ir tik aizraujoša, jo jūs varat sākt mācīties savā tempā, ērti atrodoties savās mājās.

## Kā es varu sākt?

Sāciet izpētīt dažādas jomas, lai atklātu savas intereses. Bieži vien varat sākt tikai ar datoriem vai ierīcēm, kas atrodas jūsu mājās.

- **Kodēšana**: Apgūstiet programmēšanas pamatus. Python, HTML vai JavaScript ir piemērotas valodas, lai sāktu. Apsveriet mācīties kādā tiešsaistes apmācību vietnē vai paņemiet jebkuru programmēšanas grāmatu iesācējiem.
- **Sistēmas**: Apgūstiet operētājsistēmu, piemēram, Linux vai Windows, administrēšanas pamatus. Ja patiešām vēlaties pamatīgi iedziļināties, attīstiet zināšanas, izmantojot komandrindas saskarni un skriptus.
- **Lietojumprogrammas**: Uzziniet, kā konfigurēt, palaist un uzturēt lietojumprogrammas, piemēram, tīmekļa serverus.

- **Tīklošana**: Atklājiet, kā datori un ierīces sarunājas viens ar otru, tverot un analizējot tīkla trafiku. Tas var būt ļoti jautri, jo jūsu mājās, visticamāk, jau ir tīkla vide, kurai ir pievienotas visa veida ierīces.
- **Mākoņu tehnoloģijas**: Iemācieties, kā darbojas mākoņu pakalpojumi un kā tos var izmantot dažādos veidos.

Izveidojiet savu laboratoriju mājās. Varat izmantot tiešsaistes mākoņu resursus, piemēram, Amazon AWS vai Microsoft Azure, vai arī varat izveidot vairākas virtuālās operētājsistēmas vienā fiziskajā datorā ar virtualizācijas pakalpojumiem. Ja vēlaties strādāt tieši ar aparatūru, iegādājieties vienkāršus, lētus datorus, piemēram, Raspberry Pi vai Arduino. Kad sistēmas ir izveidotas un darbojas, sāciet ar tām mijiedarboties un uzziniet visu iespējamo par to konfigurēšanu un optimizēšanu, vai sāciet programmēt un veidot kodu šajās sistēmās. Nav pareiza vai nepareiza veida, kā sākt, vienkārši sekojiet līdzi tam, kur jūs aizvedīs jūsu intereses.

Vēl viens lielisks veids, kā sākt darbu, ir iepazīties un sadarboties ar citiem kiberdrošības jomā. Apsveriet iespēju apmeklēt vietējo kiberdrošības konferenci vai virtuālu "konferenci", piemēram, Bsides vai SANS New2Cyber. Grūtākais ir atrast pirmo pasākumu vai tikšanos. Kad esat ieradies pasākumā, komunicējiet ar citiem apmeklētājiem un paplašiniet savu profesionālo tīklu.

Citas iespējas, kā apgūt kiberdrošību, ietver YouTube videoklipus, raidierakstu klausīšanos, tiešsaistes forumu apmeklēšanu, drošības profesionāļu emuāru abonēšanu vai dalību tiešsaistes Capture the Flag (CTF) pasākumos. Galu galā – neļaujiet savai izglītībai vai iepriekšējai pieredzei jūs atturēt. Galvenās īpašības ir aizrautīga mācīšanās un palīdzēšana citiem, kā arī spēja "domāt ārpus rāmjiem". Tiklīdz jūs sāksiet attīstīt savas tehniskās prasmes un tikties ar citiem, iespējas parādīsies.

## Viesredaktors

Lodrina Černe (Lodrina Cherne) (@hexplates) ir Cybereason galvenā drošības aizstāve, kas virza inovācijas un paraugprakses attīstību saistībā ar kiberdrošības standartiem un politiku. Viņa ir arī sertificēta instruktore SANS institūtā, kur viņa palīdz informācijas drošības profesionāļiem uzlabot pamata izpratni par digitālo kriminālistiku un reaģēšanu uz incidentiem (DFIR).

## Resursi

**Security Bsides konferences**: http://www.securitybsides.com/
**Sievietes kiberdrošībā (Women in Cybersecurity)**: https://www.wicys.org/
**New2Cyber YouTube atskaņojumu saraksts**: https://youtube.com/playlist?list=PLtgaAEEmVe6BQkZiJC5nIk9xx74QTGtsZ
**SANS kiberakadēmijas**: https://www.sans.org/scholarship-academies/
**SANS Cyber Aces**: https://www.cyberaces.org/
**Kiberdrošības raidieraksti**: https://www.sans.org/blog/cybersecurity-podcast-roundup/

**Tulkojums:** CERT.LV