OUCH! 2023 - 02

Ikmēneša informācijas drošības izdevums tev

Vai man ir nepieciešama drošības programmatūra?

Pārskats

Kad pirms vairākiem gadiem iegādājāties jaunu datoru, bieži vien datorā bija jāinstalē papildu drošības programmatūra, lai padarītu to drošu pret kiberuzbrucējiem. Tomēr lielākajai daļai mūsdienu datoru un ierīču jau ir iebūvēti daudzi drošības līdzekļi, piemēram, automātiskā atjaunināšana, ugunsmūri, diska šifrēšana un datņu aizsardzība. Turklāt Microsoft nodrošina Windows datoros drošības funkciju Microsoft Defender, kas ietver papildu funkcijas, piemēram, pretvīrusu programmatūru. Daudzos veidos mūsdienu sistēmas pēc noklusējuma ir daudz drošākas. Patiesībā JŪS, visticamāk, tagad esat visvājākā "vieta" datora drošībā. Tāpēc kiberuzbrucēji nepārtraukti apdraud cilvēkus, mēģinot ar viltu piespiest jūs darīt lietas, ko nevajadzētu darīt, piemēram, izpaust paroles, noklikšķināt uz saitēm vai atvērt e-pasta pielikumus, kas instalē ļaundabīgu programmatūru jūsu datorā vai izpauž kredītkartes informāciju.

Kurus rīkus vajadzētu apsvērt izmantot?

Ja vēlaties veikt papildu pasākumus sistēmu drošībai, varat apsvērt dažas papildu drošības programmas.

Paroļu pārvaldnieks: Paroles var būt sarežģītas un apgrūtinošas, īpaši tad, ja ir jāatceras, iespējams, simtiem dažādu paroļu. Paroļu pārvaldnieks ir droša krātuve, kas aizsargā un glabā visas jūsu paroles, lai jums būtu jāatceras tikai viena galvenā parole. Turklāt tas var pieteikt jūs vietnēs, ģenerēt jums paroles un palīdzēt apstiprināt noteiktas vietnes.

Virtuālais privātais tīkls (VPN): VPN galvenokārt aizsargā jūsu konfidencialitāti, šifrējot jūsu savienojumu ar internetu un slēpjot jūsu atrašanās vietu.

Drošības komplekti: Tās ir drošības programmatūras paketes, kas nodrošina drošības funkcijas papildus tām, ko jau nodrošina operētājsistēma. Piemēram, bīstamu vietņu filtrēšana, vecāku kontroles programmatūra un bieži arī VPN. Katram komplektam ir dažādas funkcijas, tāpēc izpētiet, kurš no tiem jums šķiet vispiemērotākais, ja jums tāds ir nepieciešams.

Drošības pakalpojumu sniedzēja izvēle

Ja nepieciešams iegādāties papildu drošības rīkus vai programmatūru, varat izvēlēties no dažādiem piegādātājiem. Kuru izvēlēties? Bieži vien dažādu piegādātāju piedāvātās funkcijas ir vairāk līdzīgas nekā atšķirīgas. Galvenais ir izmantot uzticama piegādātāja risinājumu. Jūs nevēlaties nejauši iegādāties un instalēt kibernoziedznieku izplatītu programmatūru, kas ir inficēta ar ļaunatūru.

Iegādājieties rīkus tikai no labi zināmiem piegādātājiem, par kuriem esat dzirdējuši un kuriem uzticaties. Nekad nepērciet rīku no uzņēmuma, par kuru neko nezināt, kurš ir pavisam jauns vai kuram nav pieejamu komentāru vai ir daudz negatīvu komentāru. Jums jābūt pārliecinātam, ka iegādājamais risinājums ir likumīgs un regulāri atjaunināts un uzturēts. Iespējams, pat jāapsver, kurā valstī atrodas piegādātājs. Ir daudzas tiešsaistes vietnes, kurās ir uzticamu piegādātāju pārskati par to drošības programmatūras funkciju un izmaksu atšķirībām.

Esiet piesardzīgi ar bezmaksas rīkiem. Lai gan ir pieejami lieliski bezmaksas drošības rīki, var rasties dažas problēmas. Šo rīku funkcijas var būt ierobežotas, tos var būt grūti izmantot vai tie var nebūt bieži atjaunināti. Dažos gadījumos bezmaksas rīkus var izstrādāt kiberuzbrucēji un pēc tam inficēt ar ļaunatūru.

Atcerieties, ka, lai gan šie drošības rīki ir noderīgi, vispirms izmantojiet datorā iebūvētās drošības funkcijas, tostarp ieslēdziet automātisko atjaunināšanu. Mūsdienu operētājsistēmas pēc noklusējuma ir ļoti drošas. Jūs esat sava labākā aizsardzība. Esiet piesardzīgi ar jebkādiem neparastiem vai aizdomīgiem tālruņa zvaniem, e-pasta ziņojumiem vai īsziņām. Neviena drošības programmatūra pasaulē nevar pasargāt jūs no tā, ka kāds mēģina jūs apmānīt vai apmuļķot, lai jūs izdarītu kaut ko tādu, ko nevajadzētu darīt.

Viesredaktors

Niko “Dutch_OsintGuy” Dekenss (Nico Dekens) ir sertificēts institūta SANS instruktors un bijušais valdības izlūkošanas analītiķis, kas specializējies publiskos avotos pieejamu izlūkdatu ieguves (Open-Source Intelligence — OSINT) jomā. Plašāka informācija par Niko atrodama šeit: https://www.sans.org/profiles/nico-dekens/ un šeit https://www.dutchosintguy.com.

Resursi

Paroļu pārvaldnieki: https://www.sans.org/newsletters/ouch/password-managers/
Atjauninājumu nozīme: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Virtuālie privātie tīkli: https://www.privacyguides.org/vpn/
Sociālā inženierija: https://www.youtube.com/watch?v=lc7scxvKQOo
Drošības komplekta apskati: https://www.pcmag.com/picks/the-best-security-suites

Tulkojums: CERT.LV