MINISTARSTVO ZA INFORMACIONO DRUŠTVO I TELEKOMUNIKACIJE

- CIRT -

SMJERNICE ZA BEZBJEDNOST I ZAŠTITU INFORMACIJA U SAJBER PROSTORU

PRINCIPI BEZBJEDNOSNE KULTURE

- SVIJEST
- ODGOVORNOST
- ODGOVOR NA INCIDENT
- ETIKA
- DEMOKRATIJA
- PROCJENA RIZIKA
- DIZAJN ZA BEZBJEDNOST I IMPLEMENTACIJA
- UPRAVLJANJE BEZBJEDNOSTI
- PONOVNA PROCJENA

BEZBJEDNOST ZAVISI OD KORISNIKA

Koncept bezbjednosti se odnosi na važnost bezbjednosti i zaštite informacija i podataka u sajber prostoru. Bezbjednosni standardi nisu tajna, već osnovni zahtjev svakog korisnika. Bez bezbjednosne kulture nemoguće je obezbijediti razvoj informacionog društva.

Prenosimo svoj rad i život u virtuelnu sferu i oslanjamo se na nju, a da toga nismo svjesni. Svijest o mogućnostima zloupotrebe informacija i informisanost o postupcima i sredstvima zaštite informacija je od velike važnosti za sajber bezbjednost.

TREBA BITI SVJESTAN DA RIZIK POSTOJI, ALI DA TREBA URADITI SVE ŠTO JE MOGUĆE, KAKO BI SE ISTI UMANJIO.

Edukacija krajnjih korisnika i dijeljenje informacija su veoma važne komponente u procesu bezbjednosti sa naglaskom na neophodnu edukaciju djece, i to od osnovne škole, jer se u tom uzrastu upoznaju sa načinom korišćenja novih tehnologija i stiču navike ponašanja u sajber prostoru.

Dobre strane interneta svakako treba iskoristiti, ali zaštita je izuzetno značajna, kako zbog privatnosti, tako i zbog sprečavanja krivičnih dijela vezanih za tehnološki kriminal.

BORBA PROTIV IZAZOVA BEZBJEDNOSTI U SAJBER PROSTORU NIJE SAMO PROBLEM STRUČNJAKA ZA BEZBJEDNOST, VEĆ SAMIH KORISNIKA KOJI TREBAJU DA PREDUZMU NEOPHODNE PREVENTIVNE MJERE, KAKO NE BI POSTALI ŽRTVE PREVARA I SAJBER NAPADA.

BEZBJEDNOST NALOGA ZAVISI OD DVA KORAKA:

1.KREIRANJA „SNAŽNE“, „JAKE“, „KVALITETNE“ ODNOSNO JEDNOM RJEČJU, BEZBJEDNE LOZINKE.
2. ČUVANJA TAJNOSTI TE LOZINKE.

RIZICI ZLOUPOTREBE PODATAKA O LIČNOSTI:

- **KRAĐA IDENTITETA.** Zloupotreba tuđih podataka o ličnosti za sopstvenu korist.
- **ZLOUPOTREBA PODATAKA O LIČNOSTI U KOMERCIJALNE SVRHE.** Neovlašćena prodaja ili ustupanje podataka o ličnosti i tvojih navika na internetu. Neželjeni mejlovi (spam) pripadaju ovoj kategoriji.
- **MALTRETIRANJE U VIRTUELNOM SVIJETU.** Jedan od koraka za prevenciju i zaštitu zloupotrebe ličnih podataka jeste da budeš obazriv prilikom dijeljenja ličnih informacija.
- **SEKSUALNO UZNEMIRAVANJE.** Dijeljenje intimnih i eksplicitnih fotografija ili video materijala može dovesti do zloupotreba.

PRIVATNOST NA INTERNETU

⇒ Razumjeti važnost i ispravan način kreiranja lozinke. Uvijek koristite kompleksne lozinke koje sadrže slova, brojeve i znakove. Lozinku treba redovno mijenjati, ne zapisivati je na papiru i ne dijeliti je ni sa kim. Ne koristiti istu lozinku za sve servise.

⇒ Prije nego pošaljete lične informacije, saznajte kako će se koristiti i da li će i kome biti proslijeđene.

⇒ Nemojte davati informacije o sebi putem telefona, preko email-ova ili internet servisa ukoliko nijeste sigurni, ili ne znate sa kim komunicirate.

⇒ Čuvajte podatke sa platnih kartica, podatke o bankovnim i drugim računima i izbjegavajte korišćenje ličnih podataka na Internetu, kao što su, npr. datum rođenja, broj telefona i slično.

⇒ Čuvajte informacije u elektronskom obliku na sigurnom mjestu, i ukoliko postoji mogućnost, na uređajima bez Internet konekcije ili na prenosivim memorijama (USB, eksterni hard disk i drugi).

⇒ Kada vršite download sa Interneta, vodite računa o tome koje podatke ostavljate prilikom registracije, pošto se ti podaci od strane izvršilaca krivičnog djela vrlo često na ovaj način prikupljaju radi njihove dalje zloupotrebe.

UOBIČAJENI SIMPTOMI ZLONAJERNOG SOFTVERA:

- Neželjena preusmjeravanja URL-ova;
- Pop up oglasi;
- Izmijenjeni Google rezultati pretrage;
- Dodatne aplikacije ili neželjene alatne trake ili bočne trake za pretraživanje u web pregledaču;
- Blokiranje antivirusne zaštite;
- Usporen rad računara.

ZAŠTITA OD ZLONAMJERNOG SOFTVERA

- **Redovno ažuriranje računara i softvera;**
- **Dobro razmislite prije nego što kliknete;**
- **Oprezno otvarajte datoteke iz e-pošte;**
- **Instalirajte antivirus.**

ZLONAMJERNI PROGRAMI

⇒ **WEB-LOKACIJE:** Potrebno je biti oprezan kada se vrši „download“, tj. kada preuzimate različite sadržaje sa Interneta na svoj računar. Kada pristupate nekoj web-lokaciji postoji mogućnost da se na njoj nalazi zlonamjerni softver koji se širi na korisnike koji pristupaju toj web-lokaciji. Neki sadržaji na Internetu osmišljeni su i napravljeni od strane izvršilaca krivičnih djela, tako da mogu da zaobiđu i najsavremeniju antivirusnu zaštitu.

Preuzimajte programe i fajlove samo sa web lokacija koje smatrate pouzdanim.

⇒ **E-POŠTA:** Potrebno je biti obazriv i svjestan potencijlnih opasnosti usljed otvaranja priloga koji sadrže makro naredbe ili izvršne fajlove. Ponekad su te poruke e-pošte samo neželjene, ali ponekad mogu sadržati štetan i zlonamjeran softver.

⇒ **DRUGI SOFTVER:** Neki programi prenose zlonamjeran ili drugi lažan softver u sklopu postupka instalacije. Prilikom instaliranja softvera pažljivo pratite okvire s porukama i pročitajte sve što je napisano sitnim slovima.

⇒ **FIZIČKI MEDIJUM:** Budite obazrivi prilikom prenošenja fajlova sa memorijskih uređaja, jer postoji mogućnost da se na njima nalazi zaražena datoteka. Prije otvaranja, skenirajte ih antivirusnim softverom.

KAKO DA ODRŽAVAM SVOJ OPERATIVNI SISTEM?

- Instaliraj pouzdan antivirus program i zaštitu od špijunskog softvera.
- Obavezno i redovno ažuriraj (patch) programe i aplikacije.
- Uključi firewall u okviru svog operativnog sistema.
- Redovno pravi bekap svojih dokumenata.

Čim posumnjate da je vaš računar zaražen, isključite ga iz mreže na koju je priključen, kao i sa internet konekcije. Spriječite da se i ostali računari zaraze, ili da u međuvremenu pokupite još neke viruse.

ANTIVIRUS I AŽURIRANJE SISTEMA

⇒ Uvijek držite uključen antivirusni program na računaru. Ova vrsta računarskog programa štiti računar od pokušaja izvršilaca krivičnih djela da pristupe računarskom sistemu, da oštete ili izbrišu Vaše podatke, otuđe korisnička imena i lozinke, ili druge osjetljive informacije.

⇒ Instalirajte i uvijek vršite ažuriranje antivirus programa na Vašem računaru. Funkcija antivirus programa je da spriječi ubacivanje računarskih virusa u računarske sisteme korisnika. Računarski virusi mogu da zaraze računar i bez znanja njegovog korisnika. Veliki broj antivirus programa može da se podesi tako da se njihovo ažuriranje vrši automatski. Povremeno napravite antivirusno skeniranje cjelokupnog sistema.

⇒ Ažurirajte operativni sistem na računaru, kako bi se ispratio razvoj tehnologije, i kako bi se sigurnosni propusti na vrjeme otkrili i uklonili. Postarajte se da računar ima najnoviju zaštitu.

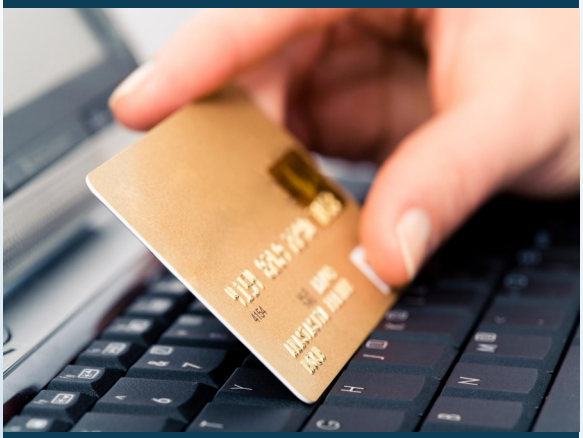
⇒ Ispraznite Registry bazu. Vaš operativni sistem skuplja podatke o programima koje koristite u Registry bazi, čak i kada uklonite programe sa računara. Za uklanjanje tih podataka, najbolje je koristiti program za čišćenje baze podataka koji se može naći besplatno na internetu. Ipak, morate biti pažljivi kod uklanjanja tih podataka, jer može se dogoditi da uklonite i više nego što treba, pa samim tim i onemogućite normalno funkcionisanje nekog drugog programa.

BEZBJEDAN WIFI

- OBAVEZNO koristiti administratorsku lozinku za svoj ruter.
- Uključi firewall na svom ruteru.
- Kad god se uključuješ na javnu WiFi konekciju, uvijek koristi zaključane/encrypted WiFi veze.
- Nikada nemoj ukucavati osjetljive informacije (važne lozinke, brojeve platnih kartica i slično) na javnim mjestima.

ONLINE KUPOVINA

- Nikada nemoj obavljati kupovine sa tuđeg računara ili mobilnog telefona.
- Obavezno koristi HTTPS verziju veb adrese onlajn prodavnica ili banaka.
- Redovno provjeravaj troškove na platnoj kartici koju koristiš za onlajn kupovinu.



BEZBJEDNOST MREŽE I SIGURNO KORIŠĆENJE VEBA

⇒ Zaštitite svoju WiFi pristupnu tačku (VPA enkripciju, promjena default-ne lozinke na ruteru, MAC filtriranje).

⇒ Zaštitite računar kada pristupate otvorenim mrežama na javnim mjestima. Preko otvorene mreže napadač može pristupiti računaru ili mobilnom telefonu, preuzeti podatke ili identitet na društvenim mrežama.

⇒ Lozinke za elektronske naloge za poštu i dr., nikada nemojte da čuvate automatski u poljima za unos. Potrebno je izabrati odgovarajuća podešavanja za omogućavanje i onemogućavanje automatskog unosa i automatskog čuvanja podataka prilikom popunjavanja obrasca.

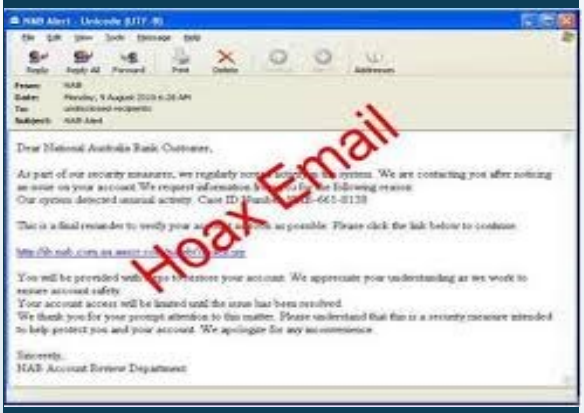
⇒ Obrisati lične podatke iz veb čitača kao što je: istorija pretraživanja, keširani internet fajlovi, kolačići, automatski unos podataka.

⇒ Onlajn aktivnosti - kada je u pitanju kupovina ili finansijske transakcije, vodite računa o tome na koju Internet stranicu se logujete, na njen izgled i sigurnosne protokole koji se na tim stranicama koriste, a koje se vrše preko sigurnih veb stranica (https lock symbol i slično). Ukoliko vršite plaćanje preko Interneta, redovno vršite kontrolu stanja na vašem računu.

⇒ Kupujte samo iz pouzdanih izvora. Za internet kupovinu, provjerite da li koristite Internet bezbjednosni protokol pod nazivom 3D Secure - Verified by Visa / SecureCode / SafeKei. Pitajte svoju banku ili izdavača kartice o tome.

KAKO SE ZAŠTITITI OD RIZIČNE UPOTREBE E-MAIL NALOGA?

- Uvijek sa rezervom pristupi svakoj e-mail poruci u kojoj se od tebe traži da upišeš svoju lozinku .
- Budi pažljiv pri svakom traženju novca ili hitnoj reakciji na neki problem, pogotovo kada su u pitanju e -mail poruke od strane nepoznatih ljudi i kompanija.
- Čuvajte se ponuda za jeftina putovanja, koje su "previše dobre da bi bile istinite".
- Klikni bezbjedno i budite svjesne/i da ne postoje besplatne usluge, uvijek dajete nešto za uzvrat.



KOMUNIKACIJE

⇒ Ograničiti pristup vašim ličnim podacima na društvenim mrežama. Što više informacija kriminalci prikupe, efikasnije mogu da planiraju napad. Potrebno je ograničiti sa kim ćete da dijelite informacije, kroz odgovarajuća podešavanja privatnosti na nalozima društvenih mreža.

⇒ Nikada ne otvarajte priloge elektronskih poruka koje su Vam stigle od osoba koje ne poznajete, i budite obazrivi kada vam stižu poruke u čijim se prilozima nalazi neželjen sadržaj koji vam neko koga poznajete šalje. Moguće je da pošiljalac koga poznajete ni sam nije svjestan šta se nalazi u prilogu poruke koju vam je proslijedio.

⇒ Čuvajte se ponuda za jeftina putovanja, koje su "previše dobre da bi bile istinite"

⇒ Budite obazrivi kada vam stigne mail sadržine da ste upravo vi dobitnik na lutriji. Nakon što se od "dobitnika" još jedan put traži da pošalje tražene podatke, željno iščekujući svoj dobitak, tzv. komisija traži plaćanje naknade, nakon čega će konačno isplatiti dobitak.

⇒ Morate razumjeti potencijalne opasnosti pri korišćenju društvenih mreža, kao što su uznemiravanje putem interneta, lažni identiteti, zaraženi linkovi ili poruke isl.

BACK-UP PODATAKA

- **USB flash memorija** (ako imate malo podataka),
- **tape drive** (za **automatski back-up**)
- **eksterni hard disk** (za **back-up cijelog sistema**).
- **online** back-up podataka

Ovi načini imaju i neke nedostatke. USB flash memorije su suviše male, lako se gube, a kao i u slučaju eksternih hard diskova, pravljenje backup-a je manuelni proces kojeg morate obavljati redovno.

ENKRIPCIJA

Ukoliko ne postoji način da se neki podatak pročita, on postaje bezvrijedan.

UPRAVLJANJE SIGURNOŠĆU PODATAKA

⇒ Nakon instalacije operativnog sistema i propratnih programa korisniku se u velikom broju slučajeva omogućava rad sa administratorskim nalogom. Najbolje je imati administratorski nalog zaštićen dobrom lozinkom, koji služi isključivo kada nešto treba instalirati, dok korisnik radi sa Guest odnosno Limited nalogom.

⇒ Enkriptovanje ili enkripcija podataka je metod zaštite podataka, kojom se šifruju podaci na hard disku i ostalim digitalnim medijima poput SSD diska, USB fleš i dr. memorijskih kartica, sa ciljem da ih sakrije od neovlašćenih lica i da, istovremeno, omogući pristup onima koji na to imaju pravo. Veoma jednostavan, a izuzetno bezbjedan koncept.

⇒ Back-up podataka je pravljenje rezervne kopije svih vaših podataka, uključujući multimediju, podatke koje ste napravili, podešavanja vašeg uređaja, imenik, e-mailove, tj sadržaje koji su nastali od kada ste prvi put pokrenuli uređaj. Potrebno je prepoznati važnost procedure pravljenja kopije podataka u slučaju gubljenja istih, finansijskih izveštaja, istorije pretraživanja isl.

⇒ Treba razlikovati brisanje i trajno uništavanje podataka. Uništavanje podataka je metoda kojom se u potpunosti uništavaju svi elektronski podaci na hard disku ili nekom drugom digitalnom mediju, kako bi se spriječilo dalje kopiranje podataka nakon što se uređaj prestane koristiti.

⇒ **Razmislite prije nego što kliknete:** Budite oprezni kod pošte i veb sajtova. Ako izgleda previše dobro da bi bilo istinito, vjerovatno je prevara u pitanju.

www.cirt.me

Zbog povećanja međusobne povezanosti, informacioni sistemi i mreže, sve su više izloženi velikom broju prijetnji i ranjivosti koje otvaraju mnoga pitanja direktno uticajući na cjelokupnu online bezbjednost.

Svi korisnici su važni akteri za obezbjeđivanje sigurnosti i treba da budu svjesni relevantnih bezbjednosnih rizika i preventivnih mjera, da preuzmu odgovornost i korake za poboljšanje bezbjednosti.

Bezbjednost informacionih sistema i mreža treba kontinuirano da se revidira, kako bi se napravile odgovarajuće izmjene u bezbjednosnoj politici, praksi, mjerama i postupcima.

Svijest o rizicima i raspoloživim mjerama zaštite je prva linija odbrane bezbjednosti informacionih sistema i mreža.

Direkcija za zaštitu od računarskih incidenata na Internetu - CIRT

cirt.me