CyberSecurity Awareness

VODIČ ZA SIGURNOST NA INTERNETU

Opasnosti sa kojima se suočavamo i savjeti za zaštitu od sajber napada

kaspersky | LANACO

februar 2024.

CyberSecurity
Awareness

4 ključna koraka

u zaštiti na internetu

- **Redovna obuka i edukacija**
- **Enkripcija**
- **Dvostruka potvrda identiteta**
- **Jaka lozinka**

Internet iz godine u godinu postaje sve opasnije mjesto i zaštita ličnih podataka je imperativ.

Osim što je nepregledno prostranstvo prepuno korisnih informacija, on je takođe i mutno more u kome vrebaju mnoge opasnosti.

Virusni napadi, malware, phishing i krađa identiteta su samo neki od načina kako naša sigurnost na internetu može biti ugrožena.
Prema **eccouncil.org**, procjenjuje se da je u 2023. godini napadnuto 33 milijarde naloga, što znači 2328 naloga dnevno, a to je 97 žrtava sajber kriminala po satu.

Mnogobrojne digitalne prijetnje nas primoravaju da se edukujemo i pripremimo plan odbrane za moguće napade.
U tu svrhu je nastao ovaj vodič u kome smo opisali glavne prijetnje i mjere zaštite na internetu.

Opasnosti sa kojima se suočavamo na internetu

Sa razvojem tehnologije, razvijaju se i opasnosti koje nam prijete iz dana u dan.

Sa svakim novim tehnološkim napretkom dolazi nova grupa sajber kriminalaca spremnih da ga iskoriste. Sajber kriminal je u ogromnom porastu u posljednjih nekoliko godina, a ova pojava ima tendenciju daljeg rasta jer su tehnologije ušle u sve pore naših života.

Ako niste nikada bili meta napada, vjerovatno ćete to u nekom momentu biti.

Trebali bismo biti svjesni svih najkritičnijih vrsta kibernetičkih prijetnji s kojima se danas suočavamo. Znanje je zaista moć, a razumijevanjem taktika sajber kriminalaca - i kako ih predvidjeti koristeći obavještajne podatke o prijetnjama – možete naučiti kako spriječiti da sigurnosni incident ugrozi vaše najvažnije informacije.

Najčešće opasnosti na internetu

Malware i virusi

Malware (malicious software) i virusi su vrste zlonamjernih softvera koji mogu nanijeti štetu računarima i mrežama.

Malware je opšti pojam koji se odnosi na bilo koji softver dizajniran s namjerom da šteti ili iskorištava bilo koji računarski sistem ili mrežu.

Ova vrsta zlonamjernog softvera se ubacuje u uređaje sa ciljem krađe ili oštećenja podataka. Obično se prenose preko email attachmenta, USB ili nekih drugih uređaja, kao i preko sumnjivih web stranica. Malware imaju i svoje podvrste: viruse, trojance, ransomware, crve, spyware i adware koji imaju različita djelovanja.

Trojanci se pojavljuju maskirani u legitimne programe, dok crvi putuju kroz mrežu šireći se na veći broj uređaja.

Spyware prikuplja informacije o korisniku bez njegovog znanja, a ransomware su malware-i koji zaključavaju naše datoteke ili računare i traže otkupninu za njihovo otključavanje.

Virus je tip malware-a koji se umnožava umetanjem svojih kopija u druge programe ili datoteke. Ključnu ulogu u odbrani od malware-a i virusa imaju provjereni **antivirusni programi.**

Distribuirano uskraćivanje usluge (DDoS)

Distributed Denial-of-Service (DDoS) napad preusmjerava uobičajeni promet servera ili mreže pretrpavajući njegovu vitalnu infrastrukturu ogromnim prilivom saobraćaja.

DDoS napadi su efikasni jer koriste više sistema i mašina - ne samo druge računare, već bilo koji uređaj povezan na internet, kao što je, na primjer, pametni TV. DDoS napadi su poput saobraćajne gužve koja blokira autoput, zaustavljajući sav normalan saobraćaj, sprečavajući ga da nastavi do svog odredišta kao i obično.

Uvođenjem preventivnih mjera i razrađenih strategija, napadi ovog tipa mogu biti izbjegnuti. Ovo su koraci koje možete preduzeti:

Učvršćivanje mreže i infrastrukture:

Potrebno je da sve softverske i hardverske komponente u mreži budu ažurirane i pravilno konfigurisane. Zaštita od DDoS napada zahtijeva implementaciju robusne, skalabilne infrastrukture i naprednih mrežnih zaštitnih rješenja, uključujući firewalle i sisteme za analizu prometa.

Sprovodite redovne sigurnosne revizije:

Redovna sigurnosna revizija mrežne strukture i web aplikacija je potrebna kako bi se identifikovale i preduhitrile ranjivosti koje bi napadači mogli iskoristiti.

Ograničite izloženost mreže:

Ograničite izloženost svoje mreže i usluga javnom internetu segmentiranjem i kontrolom pristupa.

Implementirajte ograničavanje brzine:

Kako biste ograničili broj zahtjeva koji se mogu poslati vašoj mreži, implementirajte mehanizme za ograničavanje brzine i tako spriječite napadače da preplave vaše resurse.

Phishing (fišing)

Phishing (u prevodu „pecanje“) je najučestalija opasnost na internetu, 80% svih napada se pripisuje upravo ovom načinu. U pitanju je oblik hakovanja osmišljen za preuzimanje podataka od korisnika pomoću lažnog predstavljanja. Ove prijetnje najčešće dolaze u obliku mejlova koji izgledaju kao mejlovi legitimne kompanije.

Kako bi se prepoznali ovi napadi neophodan je maksimalan oprez jer se napadači odlično maskiraju u stranicu, kompaniju ili instituciju kojoj žrtva vjeruje i kojoj će dati svoje podatke. U slučaju da unesete svoje podatke, dolazi do krađe identiteta i napadač u online prostoru nastupa pod vašim imenom.

Najbolja zaštita u ovom slučaju je edukacija kako prepoznati sumnjive mejlove i poruke. U ovim slučajevima su detalji jako važni. Potrebno je provjeriti email adresu sa koje dolazi poruka, URL stranice na koju vas navodi poruka, ali i koristiti antivirusni program koji će spriječiti sam dolazak takve poruke u sanduče.

Softver treće strane

Softver trećih strana pruža web-lokacije, alate i usluge koje su potrebne većim, popularnijim web stranicama kako bi ostale u funkciji. Najveće stranice – Google, Meta, Spotify i slične povezuju se sa stotinama softvera ovog tipa.

Međutim, ovisnost o ovom softveru također olakšava sajber kriminalcima da dođu do korisničkih podataka koje žele da iskoriste. Budući da su ove platforme trećih strana mnogo manje (i, kao rezultat toga, mnogo slabije), sajber kriminalci znaju da mogu steći ogromne količine informacija ako dobiju pristup internetskim divovima preko manje sigurnih trećih strana.

Društveni inženjering

Scareware, quid pro quo, prevare putem emaila...
svaki od ovih oblika napada socijalnog inženjeringa karakterišu taktike psihološke manipulacije koju kriminalci koriste kako bi dobili ono što žele. Žrtve bivaju prevarene i navedene da odaju svoje lične podatke i lozinke hakerima.

Socijalni inženjering je posebno efikasan protiv ljudi sa malo tehnološkog iskustva. To je zato što je ova grupa populacije daleko manje informisana o opasnostima razgovora sa strancima na mreži ili klikanja na linkove koje ne prepoznaju.

Napadi na lozinke

Često smo nemarljivi prilikom odabira lozinki i pravimo fatalne greške pri izboru, poput korištenja jedne lozinke za sve važnije naloge. Iz tog razloga, sajber kriminalci žele pristupiti jednoj od korisničkih lozinki koje se često koriste i na taj način dobiti pristup svim ostalim nalozima.

Napadač tada može promijeniti korisničke lozinke nakon što dobije pristup, pa je vraćanje naloga vlasniku težak i dugotrajan proces.

Krađa identiteta

Jedna od najvećih opasnosti digitalnog svijeta je krađa identiteta s ciljem sticanja finansijske dobiti ili pristupa određenim resursima.

Do krađe dolazi neautorizovanim pristupom i prikupljanjem ličnih podataka korisnika poput imena i prezimena, adrese, broja telefona, email adrese i sl. Metode napada su već pomenuti phishing, spyware i hakerski napadi.

Ukradeni podaci se mogu koristiti za finansijsko uništenje žrtve, kao i za oštećenje reputacije. Zaštita od napada na privatnost i krađe identiteta zahtijeva kontinuiranu pažnju i preventivne mjere kako bi se smanjio rizik od ovih zlonamjernih aktivnosti.

Mjere zaštite od sajber napada

Dobra vijest je da ne moramo biti programeri i sajber stručnjaci kako bismo se zaštitili od zlonamjernih kibernetičkih napada.

Uz dobro definisane mjere zaštite većina ovakvih napada može biti izbjegnuta. U nastavku ćemo razraditi najvažnije mjere koje pojedinac ili kompanija moraju preduzeti kako bi izbjegli krađu i oštećenje svojih podataka.

Redovna obuka i edukacija

Edukacija je broj 1 preduslov za odgovorno ponašanje na internetu. Pažljiv pristup sumnjivim web stranicama, linkovima, kao i email porukama može nas spasiti od napada zlonamjernih softvera. Edukovan korisnik će rjeđe upasti u zamku phishinga ili klikanja na zaraženi attachment, iako postoji mogućnost da se naši ranjivi sistemi zaraze malware-om bez da napravimo ikakvu grešku.

Kompanije treba da sprovode redovne edukacije u svojim timovima kako bi se ispratile sve metode sajber napada, koji se konstantno razvijaju, i kako bi se osigurao visok nivo sigurnosti podataka.

Edukacije treba da uključuju objašnjenje phishing napada, sigurno korištenje lozinki i kako prepoznati sumnjive aktivnosti.

Korisna i poželjna aktivnosti u borbi sa kibernetičkim kriminalom može biti i vodič ovoga tipa koji će pružati ažurirane informacije i savjete zaštite. Dokument ovog tipa treba da uključuje informacije o tome kako zaposleni treba da postupaju u slučaju sumnje na sajber napad.
Od izuzetne važnosti je i samo buđenje svijesti o sajber sigurnosti - postarajte se da ljudi u vašoj okolini i zaposlenici vaših organizacija ozbiljno shvate ove opasnosti.

Mnoge svjetske kompanije su posvećene dizanju svijesti o ovom problemu, pa tako organizuju i obuke iz kibernetičke sigurnosti. Jedna od njih je i **Kaspersky Automated Security Awareness Platforma.** Ova platforma je namijenjena za obuku zaposlenih čiji je cilj podizanje svijesti o bezbjednosnim rizicima u cyber svijetu i usvajanje znanja i vještina o sigurnom upravljanju i zaštiti ličnih i poslovnih podataka.

Enkripcija

Enkripcija je proces pretvaranja informacija ili podataka u kod, kako bi se spriječio neovlašteni pristup istima. Ovaj proces se također naziva kriptografija. U suštini, enkripcija omogućava da samo oni koji imaju pristup ključu (tajnom kodu) mogu čitati i razumjeti podatke.

Postoje dva glavna tipa enkripcije: simetrična i asimetrična.

Simetrična enkripcija

Koristi isti ključ za šifrovanje (enkripciju) i dešifrovanje (dekripciju) podataka. Na primjer, ako pošaljete šifrovanu poruku prijatelju, i vi i on morate imati isti ključ za šifrovanje i dešifrovanje poruke. Glavni izazov u ovom slučaju je sigurno dijeljenje ključa.

Asimetrična enkripcija

Poznata i kao enkripcija s javnim ključem, koristi par ključeva: javni i privatni ključ. Javni ključ se može dijeliti sa svima, ali privatni ključ se čuva u tajnosti. Podaci šifrovani s javnim ključem mogu se dešifrovati samo odgovarajućim privatnim ključem, i obrnuto. Ovo rješava problem dijeljenja ključeva koji postoji kod simetrične enkripcije.

Enkripcija se široko koristi u svakodnevnim aplikacijama, od sigurnosnih sistema i komunikacija preko interneta (kao što su e-mailovi i bankarski transferi) do zaštite povjerljivih informacija u vladinim i vojnim institucijama.

Enkripciju, kao vid zaštite, možete koristiti i na svojim uređajima tako što ćete podesiti nešto što se zove enkripcija cijelog diska. To znači da je cijeli uređaj šifrovan, i da ukoliko dođe do krađe uređaja, neće doći i do izvlačenja podataka.

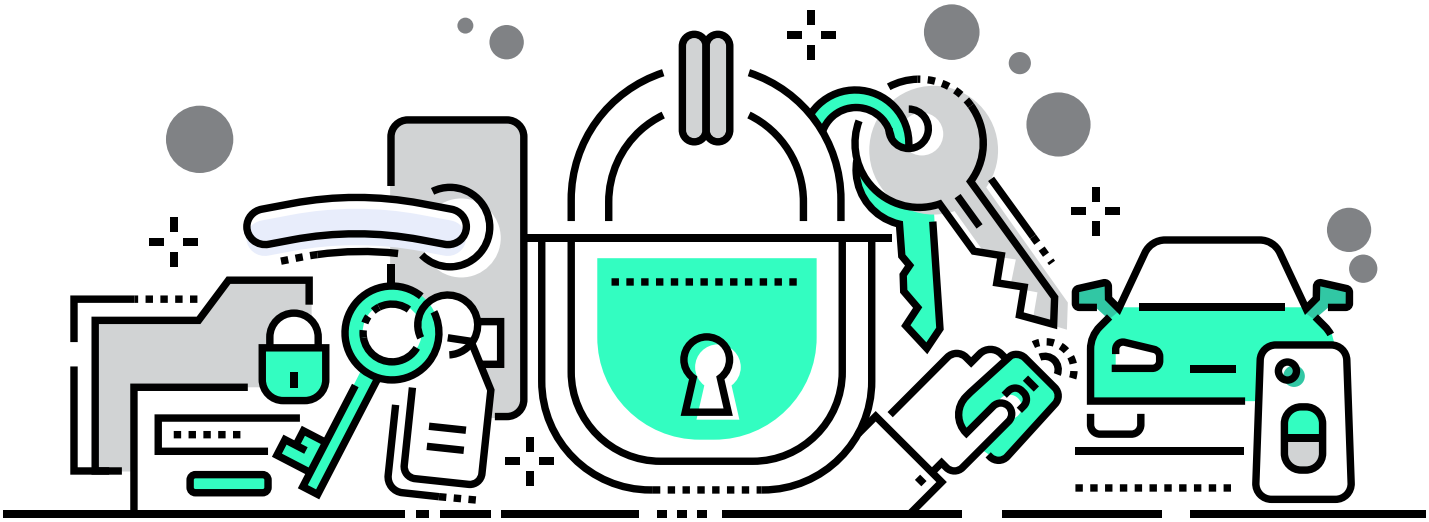
Mnogi moderni uređaji, poput pametnih telefona i računara, danas nude mogućnost enkripcije cijelog diska.

Apple - ovi uređaji, poput ajfona i ajpeda, automatski uključuju enkripciju cijelog diska prilikom kreiranja obične šifre za pristupanje uređaju, dok noviji android uređaji (od verzije 9.0 pa nadalje) imaju fabrički podešenu enkripciju, što možete provjeriti na svom uređaju.

Zašto je sigurnost uređaja tako važna? Zato što su hakeri u mogućnosti da bilježe tastere koji pritišćemo na tastaturi i da prate naše razgovore bez obzira na to koliko je aplikacija za razmjenu poruka bezbjedna, ako ocijene da uređaje koristimo za razmjenu važnih informacija.

Jaka lozinka

Digitalno doba nas je primoralo da koristimo mnoštvo servisa kako bismo funkcionisali u online prostoru. Većina nas danas ima na desetine naloga koje koristi, od Gmail naloga, društvenih mreža, aplikacija za dopisivanje, elektronskog bankarstva... Na prvoj liniji odbrane sigurnosti ovih naloga, ličnih i poslovnih, su lozinke.
Često zaboravljamo važnost lozinki i propuštamo da ih adekvatno zaštitimo. Greške u njihovom odabiru i upotrebi su najčešći razlog zbog koga dolazi do krađe podataka, jer je slabe lozinke lako probiti i zloupotrijebiti.



Šta čini jaku lozinku?

Dužina:

Kratke lozinke je lako pogoditi, posebno jer hakovanje lozinki danas vrše programi koji jednostavnim pogađanjem kombinacija dolaze do rješenja. Preporučuje se da lozinke imaju bar 16 znakova, odnosno 5 riječi.

Nasumičnost:

Za lozinke nemojte koristiti lične podatke do kojih se može lako doći jednostavnim guglanjem. Lozinka ne smije da sadrži podatke poput datuma rođenja, imena, prezimena, mjesta stanovanja i sl.

Jedinstvenost

Kombinacija nekoliko uobičajenih, ali nasumičnih riječi može biti dobra lozinka. Dodajte nizu i broj ili neki specijalni karakter (?&% i sl.) za dodatnu zaštitu. Npr. „put knjiga 20%“

Zbog količine naloga koje koristimo, radi lakšeg pamćenja, nerijetko smo skloni da odaberemo jednu lozinku koju ćemo koristiti za sve ili većinu naloga. Ovo nikako ne bismo trebali raditi jer sve što je potrebno jednom hakeru u tom slučaju je da pogodi tu jednu lozinku i otvaraju mu se vrata naše privatnosti i online podataka.

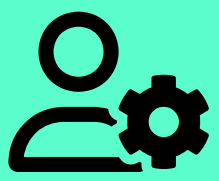
Kako biste riješili problem pamćenja svojih lozinki, a pritom ih i zaštitili, koristite Password Manager koji će, po potrebi, za vas generisati jaku lozinku, čuvati je i ispisati tamo gdje je potrebno. Na ovaj način, pamtićete samo jednu glavnu lozinku koja čuva sve ostale.

Aplikacije poput Password Managera konstantno rade na usavršavanju sigurnosti i dizajnirane su tako da ne mogu otključati vaše naloge, pa u slučaju da su hakovane, vaši podaci nisu izloženi riziku.

Ipak, ako ste pomislili da je sa čuvanjem lozinki u pretraživaču ista stvar, varate se. Pretraživači poput Chrome, Firefox-a ili Safarija nemaju isti nivo sigurnosti. Ukoliko čuvate lozinke u pretraživaču, obrišite ih.

Još jedna od predostrožnosti koju treba uzeti u obzir je redovno mijenjanje lozinke. Ovo posebno vrijedi za osjetljive naloge, poput email-a ili naloga za elektronsko bankarstvo, za koje biste trebali mijenjati lozinku svakih šest mjeseci.

Dodatna zaštita za vaše lozinke je dvostruka potvrda identiteta.



Dvostruka potvrda identiteta

Two-factor authentication (2FA) je metoda sigurnosne verifikacije koja zahtijeva dva različita oblika identifikacije kako bi se pristupilo nalogu ili sistemu.
Ovaj pristup je značajno sigurniji od tradicionalne lozinke, jer zahtijeva dva različita tipa dokaza (faktora) da je korisnik onaj ko tvrdi da jeste.

Ovi faktori obično spadaju u tri kategorije:

Znanje:

Nešto što korisnik zna, poput lozinke ili PIN koda.

Posjedovanje:

Nešto što korisnik ima, kao što je mobilni telefon (na koji se može poslati SMS sa kodom) ili token uređaj.

Inherentnost:

Nešto što je inherentno korisniku, poput otiska prsta ili skeniranja lica.

Kod dvostruke potvrde identiteta, korisnik mora pružiti dokaz iz dvije od ove tri kategorije. Na primjer, korisnik može unijeti svoju lozinku (znanje) i zatim unijeti kod koji je primljen na mobilni telefon (posjedovanje). To značajno smanjuje rizik od neovlašćenog pristupa, jer čak i ako neko drugi sazna lozinku, neće moći pristupiti nalogu bez drugog faktora. Tamo gdje je moguće, obavezno uključite dvostruku potvrdu identiteta.

Tri najčešće metode za 2FA su sigurnosni ključevi, aplikacije za potvrdu identiteta i jednokratni brojevi za autorizaciju koji se šalju SMS-om.

Sigurnosni ključevi su vjerovatno najbolja opcija jer su neprobojni za phishing napade. U pitanju su mali hardverski tokeni nalik na USB uređaje koje možete uvijek nositi sa sobom ili držati uključene u računar. U slučaju probijanja lozinke, drugi korak potvrde identiteta je upravo sigurnosni ključ.

Druga opcija su aplikacije za potvrdu identiteta poput Google Authenticator, Authy i Duo Mobile. Ove aplikacije na vašem uređaju generišu jednokratni kod, koji je obično kratkotrajan, što znači da važi samo nekoliko sekundi ili minuta.

Najučestaliji tip dvostruke potvrde identiteta, ali i najmanje siguran, su brojevi koji se šalju preko SMS poruka. Takođe su u pitanju kratkotrajni kodovi kojima potvrđujete identitet, ali njihova veća ranjivost je u tome što se SMS poruke mogu presresti, a brojevi telefona mogu biti lažirani ili hakovani preko mobilnih operatera.

Ukoliko želite da uključite 2FA, **na ovoj stranici** možete pronaći informacije kako da to uradite na određenom servisu (kao što je Gmail, Facebook, Office 365, X...).

Softveri za sajber sigurnost

Kako su napadi iz godine u godinu sve učestaliji i sofisticiraniji, antivirusni i drugi softveri za sajber sigurnost postali su još važniji.Dostupni su mnogi alati od kojih svaki ima svoje jedinstvene karakteristike i prednosti, uključujući:

BitDefender

je vodeći dobavljač sigurnosnih rješenja za kompanije i pojedince širom svijeta. Kompanija nudi različite proizvode i usluge, uključujući antivirusni softver, internet sigurnost, uklanjanje zlonamjernog softvera i alate za modeliranje prijetnji. BitDefender pruža nekoliko usluga obavještavanja o prijetnjama, uključujući mapu globalnih prijetnji u stvarnom vremenu i online skener prijetnji.

SolarWinds:

Ovaj alat na sveobuhvatan način pregleda sigurnosni položaj kompanije ili organizacije. Omogućava korisnicima da vide sve potencijalne prijetnje, a zatim preduzmu korake da ih ublaže.

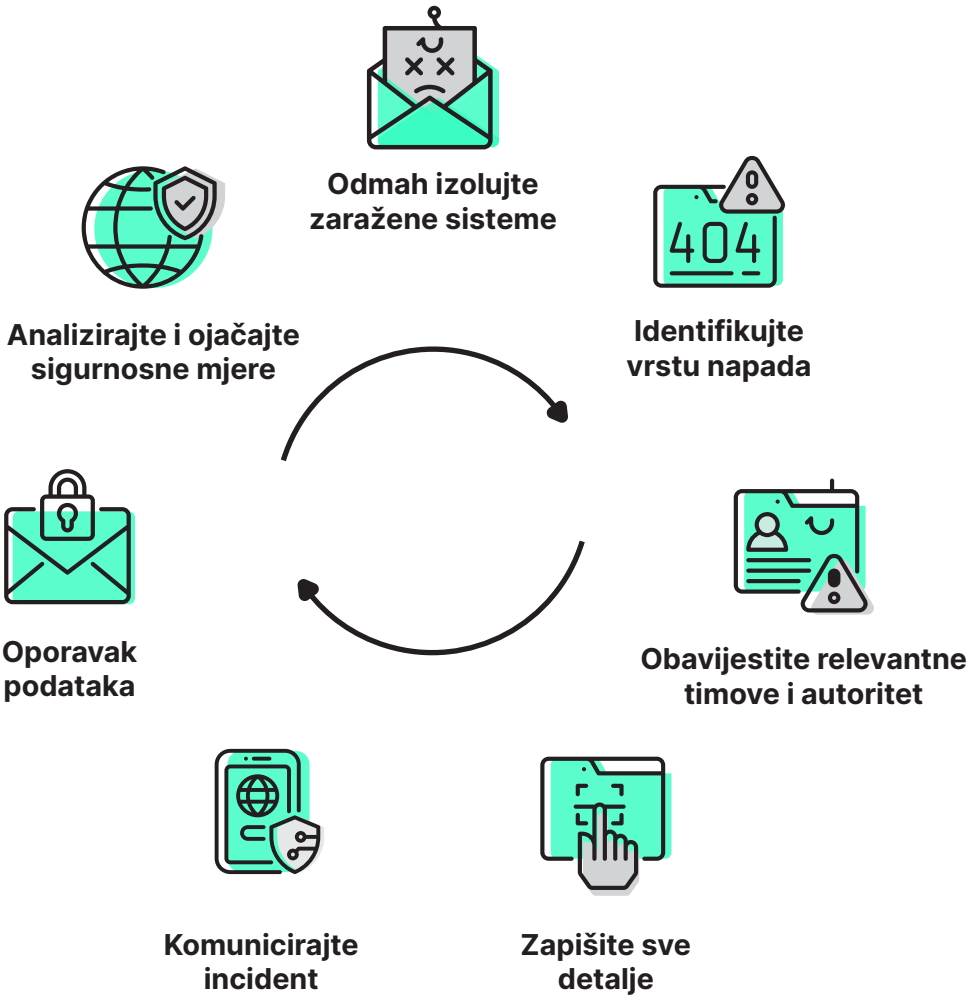
CrowdStrike:

Ovaj alat pruža organizacijama trenutnu vidljivost svih aktivnosti na njihovoj mreži. Pomaže im da brzo i efikasno prepoznaju prijetnje i odgovore na njih.

Kasperski takođe nudi, osim antivirusnih programa, i zaštitu od hakerskih napada (blokira prevarantske email poruke, zaražene reklame i programe za krađu podataka kreditne kartice), kao i alatke protiv softvera koji traže otkup (zaustavlja sve napade prije nego što se dogode).

Kako treba postupati u slučaju sajber napada?

U slučaju da vam se desi sajber napad, potrebno je preduzeti mjere kako se zlonamjerno djelovanje napadača ne bi širilo dalje. Evo šta možete učiniti u tom slučaju:



Odmah izolujte zaražene sisteme
Kako biste spriječili širenje napada, odmah izolujte zaražene ili sumnjive sisteme od mreže. Ovo može uključivati isključivanje računara, odvajanje od Wi-Fi mreže ili fizičko uklanjanje mrežnih kablova.
Identifikujte vrstu napada
Pokušajte identifikovati koja vrsta sajber napada je u pitanju (npr. ransomware, phishing, DDoS napad).
Različiti tipovi napada zahtijevaju različite reakcije.
Obavijestite relevantne timove i autoritet
Obavijestite interne timove zadužene za IT sigurnost i menadžment. U nekim slučajevima, kao što su data breaches, može biti potrebno obavijestiti i vanjske autoritete, kao što su policijske službe.
Zapišite sve detalje
Zabilježite sve što znate o incidentu, uključujući kako je otkriven, koji su sistemi zahvaćeni, i bilo koje druge relevantne informacije. Ovo može pomoći u istrazi i oporavku.
Komunicirajte incident
Informišite zaposlene i, ako je potrebno, klijente o incidentu. Važno je biti transparentan o tome šta se dogodilo, ali i oprezan da ne otkrivate previše tehničkih detalja koji bi mogli ugroziti daljnju sigurnost.
Oporavak podataka
Ako je to moguće, pokušajte oporaviti izgubljene ili oštećene podatke koristeći backupove. Ako ste bili žrtva ransomware napada, razmotrite mogućnosti prije plaćanja otkupnine (što često nije preporučljivo jer ne garantuje vraćanje podataka).
Analizirajte i ojačajte sigurnosne mjere
Nakon što je incident riješen, sprovedite temeljnu analizu kako bi se utvrdilo zašto se napad dogodio i koje mjere sigurnosti treba poboljšati kako bi se spriječili budući napadi.

Savjeti za sigurnost djece na internetu

Djeca su najranjiviji segment društva, kako u digitalnom, tako i u analognom svijetu. Generacije koje odrastaju u eri rapidnog tehnološkog napretka su izložene nebrojenim opasnostima od kojih ih moramo zaštititi.

Prema istraživanju kompanije Kasperski, lidera iz oblasti sigurnosti, 70% djece širom svijeta provede najmanje 3-5 sati na svojim digitalnim uređajima. Navike odraslih se prenose na djecu, iako djeca nemaju isti nivo svijesti po pitanju sigurnosti i internet je za njih daleko opasnija stvar. Važno je uspostaviti zdrave digitalne navike kako bi iste djeci bile samo na korist, a ne i na štetu.

Roditeljima je često potrebna pomoć u zaštiti djece na internetu i zato je Kasperski osmislio **Safe Kids program** koji im omogućava da nadgledaju, zaštite i edukuju svoju djecu.
Pored sigurnosnog programa koji štiti djecu na internetu postoje i drugi koraci koje je potrebno preduzeti kako bi vaše dijete bilo sigurno kada koristi internet.

Obrazovanje i komunikacija:

Prvi korak je edukovati djecu o potencijalnim opasnostima na internetu. Razgovarajte otvoreno o temama kao što su sajberbuling, prevare, i neprimjereni sadržaj. Objasnite im važnost očuvanja privatnosti i zašto ne bi trebali dijeliti lične informacije online.

Postavljanje pravila:

Postavite jasna pravila o tome što se smije a šta ne smije raditi na internetu. To može uključivati ograničenja na vrste web stranica koje mogu posjetiti, s kime mogu komunicirati, i koliko vremena mogu provesti online.

Korištenje roditeljskih kontrola:

Većina operativnih sistema, pretraživača, i aplikacija nudi opcije roditeljske kontrole koje vam omogućavaju da ograničite pristup određenim sadržajima, postavite vremenska ograničenja, i pratite aktivnosti na internetu.

Upotreba sigurnih pretraživača i aplikacija:

Postoje pretraživači i aplikacije dizajnirani specifično za djecu, koji nude sigurnije online iskustvo s unaprijed filtriranim sadržajem.

Zaštita privatnosti:

Naučite djecu važnosti zaštite njihovih ličnih podataka. To uključuje informacije poput imena, adrese, brojeva telefona, škole koju pohađaju, i slično.

Oprez s društvenim mrežama:

Društvene mreže mogu biti veliki izvor opasnosti za djecu. Ograničite ili nadgledajte njihovo korištenje društvenih mreža i edukujte ih o sigurnom ponašanju na tim platformama.

Redovno nadgledanje i praćenje:

Periodički provjeravajte aktivnosti vašeg djeteta na internetu. To ne znači neprestano špijuniranje, već održavanje svijesti o tome šta rade online.

Sigurnost uređaja:

Osigurajte da su svi uređaji koje vaše dijete koristi zaštićeni lozinkama i važećim antivirusnim softverom.

Podsticanje otvorenih razgovora:

Kao i o svemu drugom, podstičite dijete da s vama razgovara o bilo kakvim problemima ili neugodnim iskustvima koja su imali online.

U sklopu kampanje Cyber Security Awerness i nastojanju širenju svijest o digitalnoj bezbjednosti, slatki mali psić je tu da nam sugeriše da opasnost na prvi pogled ne mora biti očigledna.

Budite dio kampanje i pratite Lanaco društvene mreže jer kroz dijeljenje korisnih savjeta, resursa i upotrebu hashtaga **#CyberSecurityAwareness,** zajedno možemo podizati svijest i jačati otpornost na digitalne prijetnje.

@lanacocompany

kaspersky | LANACO