www.vulkani.rs
office@vulkani.rs

Naziv originala:
Dr. Eric Cole
ONLINE DANGER

Original English language edition published by Morgan James Publishing

ISBN 978-86-10-04019-7

Ova knjiga štampana je na prirodnom recikliranom papiru od drveća koje raste u održivim šumama. Proces proizvodnje u potpunosti je u skladu sa svim važećim propisima Ministarstva životne sredine i prostornog planiranja Republike Srbije.

ONLAJN OPASNOST

DR ERIK KOL
STRUČNJAK ZA BEZBEDNOST
NA INTERNETU I SAJBERNINDŽA

Kako zaštititi sebe i voljene
od zle strane interneta

Prevela Radojka Jevtić

VULKAN
IZDAVAŠTVO

Beograd, 2021.

Ova knjiga je posvećena svim vrednim policajcima koji neumorno rade da nas zaštite od opasnosti koje vrebaju u stvarnom svetu i sajberprostoru

SADRŽAJ

Cela ova knjiga fokusirana je na bezbednost i znanje potrebno da vam pomogne da zaštitite sebe, porodicu i kompaniju. Svako poglavlje sadrži korake koje možete preduzeti da umanjite šanse da vas neko ugrozi.

UVOD

Ovog trena.

Želimo sve odmah i sad.

Naš svet se toliko brzo prilagodio mogućnostima interneta da ne samo da želimo sve već zahtevamo da to bude istog trena. Možda bi informacione tehnologije trebalo preimenovati u instant tehnologije.

Nema više gledanja bolno sporog učitavanja podataka, beskrajnog čekanja da razgovarate s korisničkom podrškom ili proveravanja stanja na kreditnoj kartici kada stigne pošta.

Ali da li se ponekad osećate kao da je vaš put na informacionom auto-putu malo previše rizičan, a da vi niste svesni svih onlajn-opasnosti?

Moj put u sajberprostor počeo je dok sam rastavljao svaki uređaj koji bih našao u kući, čim bi mama okrenula leđa. Uvek sam želeo da znam kako šta funkcioniše, i ako sam usput nepovratno upropastio budilnik ili blender, verujte, vredelo je.

To me je odvelo u skriveni svet informacija, do korporativnih sala širom sveta. Uglavnom radim s donosiocima odluka i upravnim odborima. Moj kontakt s tipičnim korisnicima tehnologije obično je ograničen na moje prijatelje i porodicu, koji me preplavljuju pitanjima o raznim temama, od podešavanja video-rekordera, preko instaliranja antivirusa, do neprimetnog praćenja aktivnosti dece na internetu.

To me je zapravo i inspirisalo da napišem ovu knjigu. Sajberbezbednost korisnika nije teško postići. Ne treba vam diploma iz računarskih nauka da biste zaštitili svoju porodicu i sebe. Ova knjiga je zato puna konkretnih saveta i proaktivnih uputstava čiji je cilj da učine digitalni svet bezbednijim za sve korisnike.

Želim s vama da podelim svoje znanje o sajberprostoru, da bismo mogli svi da uživamo u pogodnostima tehnologije, ali i da značajno umanjimo rizike po bezbednost koje nova tehnologija donosi.

Sajberprostor je veoma opasno mesto i svi zaslužuju da budu sigurni kada ulaze u digitalno carstvo. Budite ratnik u sajberprostoru, kanališite svog unutrašnjeg nindžu.

I ako ikada osetite da tehnologija previše brzo juri napred, molim vas, pobrinite se da su vaša deca potpuno obezbeđena.

Verovatno mislite da ne znam mnogo o roditeljstvu ako verujem da je deci teško da se prilagode novoj tehnologiji. Imam troje dece i više puta sam ih video kako uče da se snalaze s novom aplikacijom ili rešavaju prost programerski problem pre nego što ja uopšte i stavim naočare za čitanje. Međutim, iako deca brzo pokupe *kako* se nešto radi, često ne shvataju *zašto* se to radi. Ipak su to deca.

Roditelji i nastavnici zato moraju stalno da drže korak s novim tehnologijama, i zbog sebe, ali i da bi mogli da vode decu kroz sajberprostor bezbedno.

Dozvoliti deci da imaju pametne telefone, električne uređaje i računare i da budu povezani na internet bez nadzora, strukture ili discipline predstavlja recept za katastrofu. Kao odrasli, moramo da im pružimo primer, objasnimo šta je dobro, a šta loše, i da im zaplenimo telefone i računare ako se ponašaju opasno na internetu.

Sajberprostor je prava revolucija, i to ne samo što se tiče tehnološkog aspekta. Takođe predstavlja i kriminalnu revoluciju. Zamislite da najgorim kriminalcima date razne supermoći: mogućnost da preskoče kontinente u milisekundi, ogrtač nevidljivosti i beskrajne resurse. U

isto vreme, institucije nemaju dovoljno finansijskih sredstava i stalno kaskaju s pravnom regulativom i kod kuće i u inostranstvu.

Ako mislite da najgori sajberzločin koji može da se desi jeste to da vam neko ukrade broj kreditne kartice, grdno grešite. Svi misle da se loše stvari dešavaju drugim ljudima – dok se i njima nešto ne desi.

Što pre shvatite da vam je potrebna strategija za sajberbezbednost, pre ćete biti zaštićeni. Svi u sajberprostoru su potencijalna meta.

Daću vam jedan veliki insajderski savet. Ako vam je bezbednost u sajberprostoru ugrožena, postoji vrlo lak način da pronađete krivca.

Pogledajte u ogledalo!

Sada ste ili veoma zbunjeni, ili ljuti. Ako niste IT stručnjak (a većina ljudi koji čitaju ovu knjigu nisu), verovatno mislite da nikako ne može biti vaša krivica ako neki hakeri upadnu u podatke neke velike trgovinske kompanije i uzmu na milione brojeva kreditnih kartica.

Međutim, svako od nas je lično odgovoran za vaganje koristi sajberprostora i mnogih rizika. Ako koristite usluge internet bankarstva, morate da odlučite da li je korist automatskog plaćanja računa vredna potencijalnih problema: recimo, da vam ukradu sav novac s računa. Ako rado delite lična dostignuća s prijateljima i porodicom na društvenim mrežama, razmislite o mogućim posledicama ako vaše objave zapadnu za pogrešno oko.

Odgovorni digitalni građanin zna da je sam zadužen za svoju sajberbezbednost. Što nas dovodi do još jedne stavke. Ponekad ljudi donose zaista loše odluke na internetu. I to neverovatno loše. Pa, kada vaš šef sazna za neki vaš užasan komentar, koji ste o njemu ostavili na društvenim mrežama, nemojte kriviti komplikovana podešavanja privatnosti. Sami ste krivi.

U ovom trenutku je za većinu nas postalo skoro nemoguće da siđemo s internet auto-puta. To prosto nije praktično. A srećom, nije ni neophodno. Postoje mere koje možete da sprovedete da biste umanjili rizik i zaštitili sebe, svoju porodicu i svoj posao u sajberprostoru.

Kao što sam već spomenuo, mene moja porodica i prijatelji pitaju kada im treba pomoć u vezi sa sajberbezbednošću. Moja deca, kolege i prijatelji pružaju mi perspektivu da se u sajberbezbednosti ne radi samo o brojevima, milionima ukradenih kreditnih kartica ili ukradenih hiljadu dolara s računa. Svaki podatak koji je kompromitovan i svaki nalog koji je hakovan predstavlja jednu živu osobu.

I zaista se brinem za njihovu bezbednost – a i za vašu. Pridružite mi se dok vam pokazujem kako da plovite bezbedno sajberprostorom i možda ubacite i koju nindža fintu na tom putu.

GLAVA 1

NOVI SVETSKI POREDAK

Da li trošite više na kafu i kolače u „Starbaksu" nego na sopstvenu sajberbezbednost? I generalno, šta vam je važnije? Kada uzimate u obzir svoju sajberbezbednost i bezbednost vaše porodice, da li naručujete late s obranim mlekom ili dupli espreso?

U svetu koji se menja neverovatnim tempom, sjajne tehnološke inovacije dešavaju nam se pred očima. Kako napreduju lični elektronski uređaji, često se zapitam kako smo uopšte preživljavali bez telefona, tableta i računara? Kako li smo ispunjavali dane, noći i vikende?

Moji tinejdžeri provode većinu vremena na telefonu, tako uglavnom i komuniciraju s prijateljima. I tinejdžeru ništa nije tako strašno kao kad mu za kaznu oduzmete telefon. Kada oduzimate telefone tinejdžerima ili deci, kao da im oduzimate identitet i samo njihovo

postojanje. Današnja deca nemaju pojma šta da rade, a još strašnije, ni kako da funkcionišu bez elektronskih uređaja.

Shvatali mi to ili ne – a većina dece toga nije svesna – zbog svih ovih uređaja živimo u potpuno povezanom svetu, u kom skoro svaki naš pokret ostavlja neki digitalni otisak. Lako je fokusirati se na nove i bolje funkcionalnosti u tom povezanom svetu, ali takođe moramo da uzmemo u obzir i nove opasnosti koje idu uz tehnološki napredak.

Iza svakog imejla, svakog sajta, svakog paketa informacija koji vaš računar primi, vreba mogućnost zlonamernog koda, s potencijalom da vam sruši ceo svet. Na koncu vise vaš ugled, ozbiljne zakonske sankcije i ogroman finansijski gubitak, pa čak i sam vaš identitet je pod pitanjem. Ustanovljen je novi svetski poredak, a ako niste spremni za njega, lako možete postati žrtva sajberkriminala.

Organizacije u Rusiji, Kini i drugim mestima rade svaki dan po ceo dan da sakupe i iskoriste vaše digitalne informacije. Odavno je prošao tren da se zapitate da li želite da budete meta. Ako se ne bavite aktivno svojom sajberbezbednošću, vaš odgovor na to pitanje je već DA.

Većina nas nedovoljno radi na zaštiti u digitalnom svetu. Iz iskustva mogu da vam kažem da naši sajberprotivnici igraju veoma efikasnu ofanzivu. Ako niste spremni da reagujete – ili još bolje, da im se aktivno suprotstavite efikasnom odbranom – izgubićete, a gubici mogu biti znatni. Ova knjiga će vas naučiti kako da osmislite žestoku sajberodbranu.

PERCEPCIJA BEZBEDNOSTI

Kada upoznajem ljude na žurkama ili aerodromima i kada me pitaju šta radim, kažem im da se bavim sajberbezbednošću. Mnogi mi kažu da to mora da je najbolji posao na svetu. Ali nisu sve reakcije

pozitivne. Pre petnaest godina dobijao sam veoma čudne poglede na taj isti odgovor, kao da sam smrdljivo dete u školskom autobusu.

Ranije se verovalo da je sajberbezbednost potrebna samo vladinim institucijama s poverljivim informacijama ili velikim kompanijama s poslovnim tajnama koje treba štititi. Međutim, danas svima – svakom pojedincu u svakom dobu – treba sajberbezbednost, i smatram da sam blagosloven što radim u industriji koja pomaže da svet bude bezbednije mesto.

Ako niste uvereni da svima treba sajberbezbednost, molim vas, uključite televizor ili kupite novine i pročitajte najskorije – i tekuće – izveštaje o prodorima u baze podataka. Nijedna kompanija ili vlada više nije potpuno imuna na današnje sajberkriminalce; izgleda da svaki aspekt trgovine ili komunikacije vlade ili nekog globalnog entiteta može biti kompromitovan. I da li ste spremni za najstrašniju informaciju? Većina prodora prođe neprimećeno jer ih ne prijavljuju, tako da ono što vidite ili pročitate odražava samo mali deo problema.

Mi koji radimo u oblasti sajberbezbednosti zovemo ovu percepciju bezbednosti efektom sante leda. Ono što vidite iznad vode predstavlja samo mali procenat sveukupnog problema jer se većina sante krije pod vodom, nevidljiva i opasna. Stanje sajberbezbednosti izgleda loše, ali kao i u slučaju sante leda, problem je zapravo mnogo gori nego što većina ljudi može i da zamisli.

Uprkos više od dvadeset godina ubrzanih tehnoloških promena, prosečna osoba tek u poslednje vreme počinje da prepoznaje sajberbezbednost kao problem na koji mora da obrati pažnju. Opasnost pri onlajn-interakcijama postoji oduvek, ali problemi tek sad poprimaju razmere epidemije. Koliko god da imate godina, kakvo god da vam je iskustvo i gde god da se nalazite na svetu, ako koristite elektronske uređaje, morate da pazite na sajberbezbednost – i ova knjiga je napisana za vas.

ZBOG POGREŠNE PERCEPCIJE POSTAJETE META

Procurele fotografije sa telefona poznate osobe. Procureli imejlovi predsedničkog kandidata. Sramne poruke koje ostavlja prestolonaslednik. Samo poznate osobe su meta hakerskih napada, zar ne?

NE!

Baš kao i poznate osobe, i vi posedujete račun u banci, kreditnu karticu i popunjavate onlajn-obrasce za kupovinu – i time stvarate digitalne podatke na razne načine. Ti lični podaci predstavljaju vaš elektronski identitet. A oni su neprocenjivi, bez obzira na to kome pripadaju.

Rečnik sajberbezbednosti uključuje i termin *žetva*. Mislite o svom sajberprotivniku kao o farmeru. Sajberkriminal je rizičan posao i neće svako seme dati usev koji donosi profit. Ali baš kao i u poljoprivredi, što je žetva bogatija, to je šansa za profit bolja.

Možda je jednom farmeru previše da se brine o ogromnom polju, a tako je i sa sajberkriminalom. Ako se polje podeli na manje delove i na različite poljoprivredne kulture, lakše će se žnjeti. Ta strategija važi i za hakere.

Veštim sajberlopovima može uspeti da upadnu u veliku organizaciju i ukradu 5.000.000 podataka. Ali to nije tako lako jer velike kompanije postavljaju snažnu odbranu. S druge strane, većina pojedinaca nema obezbeđenje koje im štiti onlajn identitete i sredstva, pa je hakerima mnogo lakše da upadnu u 5.000.000 individualnih računara i ukradu lične podatke. Rezultat je isti: veliki dobitak za sajberkriminalce, a veliki gubitak za njihove žrtve.

Sajberkriminalci takođe vole takozvane *napade oko pojila*. Hakeri napadaju velike sajtove koje posećuju milioni ljudi na dnevnom nivou i infiltriraju se nakratko u njihovu odbranu. Čak i kada je veliki sajt kompromitovan na samo šezdeset minuta, to zapravo predstavlja veliku žetvu za sajberlopove.

Kad god uđete u sajberprostor, ko god da ste, zlo vreba i morate da budete spremni.

I umesto da problem bude rešen poboljšavanjem sajberodbrane, nove opasnosti i izazovi svakodnevno se umnožavaju.

Pre dvadeset godina radio sam na slučaju u kom je 10.000 podataka ukradeno (to jest, podaci kreditnih kartica i lični podaci), što je tad smatrano velikim incidentom. Rekao sam tad prijatelju da ćemo biti u ozbiljnom problemu ako dođemo do tačke da neko uspe da ukrade 100.000 podataka odjednom.

Nekoliko godina kasnije, dok sam radio na slučaju ukradenih 100.000 podataka, to je postalo uobičajeno, pa sam tad izjavio da bi milion ukradenih podataka značilo da je situacija potpuno van kontrole. Samo nekoliko godina kasnije, dostigli smo taj broj. Ipak, nisam odustajao. Tvrdio sam da će tek na desetine miliona ukradenih podataka voditi u haos. I naravno, to se nekoliko godina kasnije desilo, a danas je milijardu ukradenih podataka nova normalnost.

Lako je okriviti treću stranu – banke, prodavnice, vladu – što ne štiti vaše podatke. I zaista, te institucije i kompanije jesu odgovorne za to. Međutim, na kraju krajeva, svi mi, svaki pojedinac, mora prihvatiti odgovornost za zaštitu svojih ličnih podataka.

Kada vaš identitet i lični podaci budu kompromitovani, vi ćete morati da se nosite s posledicama. Ne kreditni biro, prodavac ili vladina agencija – iako mogu da preduzmu neke korake da vam pomognu da se oporavite. Ipak, ako želite da pobedite u sajberprostoru, VI morate da preuzmete odgovornost za sopstvenu zaštitu i da se obezbedite još danas.

ODBRANA PO DUBINI

Nijedno rešenje ne donosi potpunu bezbednost. Taj hronični nedostatak potpune zaštite i održava industriju sajberbezbednosti, koja danas vredi milijarde dolara, jer sajberprodori stalno nadmašuju preporuke korisnicima.

Ja sam još davno skovao izraz: „Prevencija je najbolja, ali je i detekcija neophodna." I zaista, ne možete sprečiti sve hakerske napade, ali trebalo bi da vam cilj bude da ih znatno smanjite i da možete da kontrolišete štetu. Možete početi tako što ćete sprovesti razne tehnike odbrane, kao što je zaštita krajnje tačke, ali takođe morate da shvatite da te mere – i to sve – iskusni sajberkriminalci uvek mogu zaobići. Uvek morate biti na oprezu kako biste prepoznali znake napada. Kada primetite neobičnu aktivnost na svom uređaju, ne ignorišite je – odmah delajte.

Dok prolazite aerodromom, često vidite znake koji vam poručuju: „Ako vidite nešto, recite nešto." Ista ta filozofija važi i za ličnu zaštitu. Ako vidite čudnu aktivnost, pozovite banku ili kompaniju koja je izdala karticu i proverite sumnjive transakcije. Što pre primetite upad i nešto preduzmete, to bolje možete da kontrolišete štetu, pa čak i da je predupredite.

Odbrana po dubini je još jedan uobičajen termin u sajberbezbednosti i on znači da aktivno preduzmete odbrambene korake da zaštitite svoj sistem. Suština je u diverzifikaciji portfolija.

Uzmite u obzir svoj penzioni fond ili neki drugi račun: nijedan pametan investitor ne stavlja 100% svojih sredstava, pa čak ni 90%, u jedan fond – jer to bi bilo previše rizično. Umesto toga, investitori diverzifikuju svoj portfolio, pa ako jedan fond propadne, druge investicije umanjuju udar na celokupne investicije.

Kada pomislite na bezbednost, morate da identifikujete više nivoa zaštite i da nikada ne zavisite samo od jednog mehanizma. Pomislite na moguće slojeve fizičke zaštite samog vašeg doma: možda živite u ograđenoj zajednici, imate alarm i imate velikog psa Fida, koji šeta po