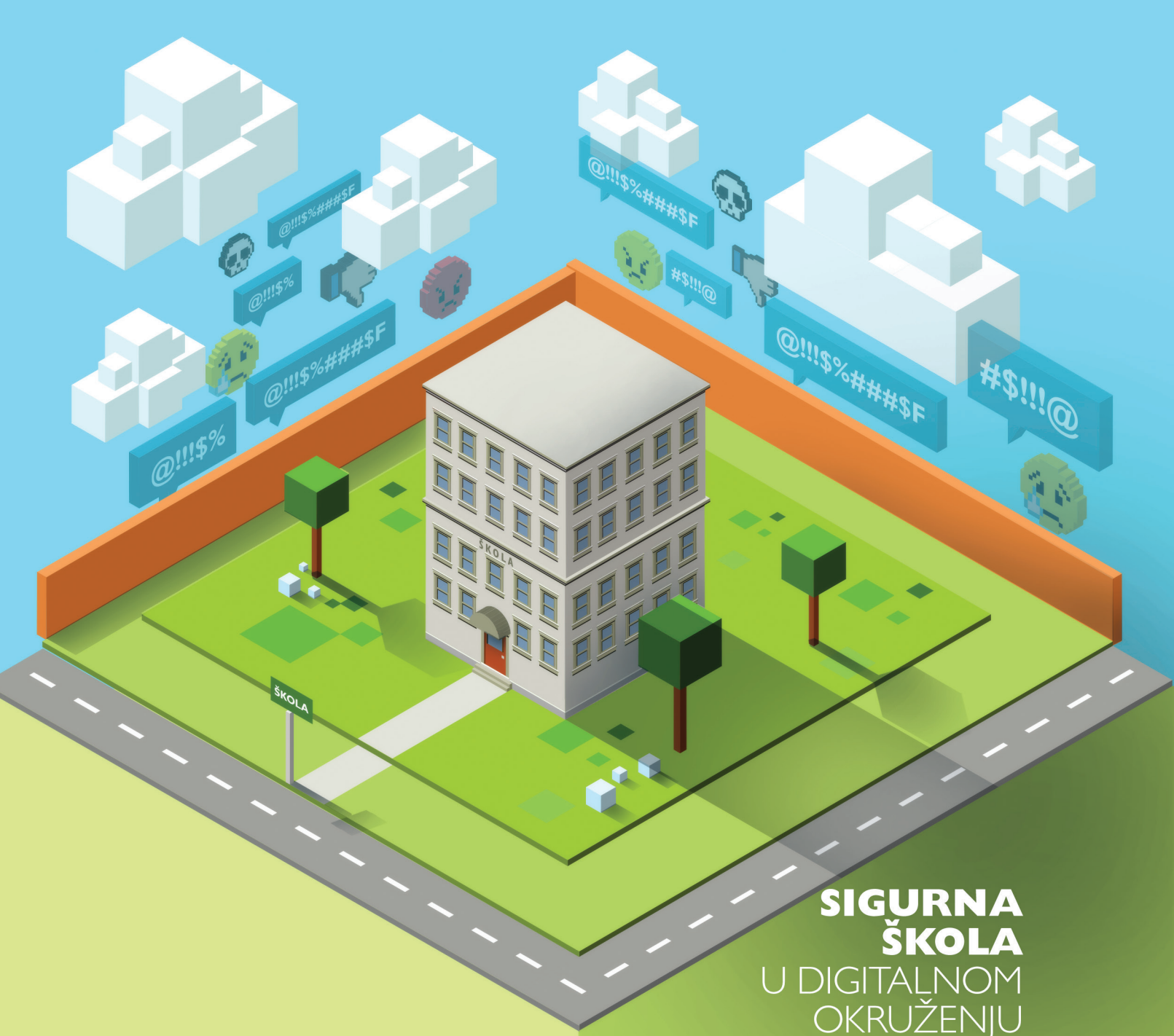


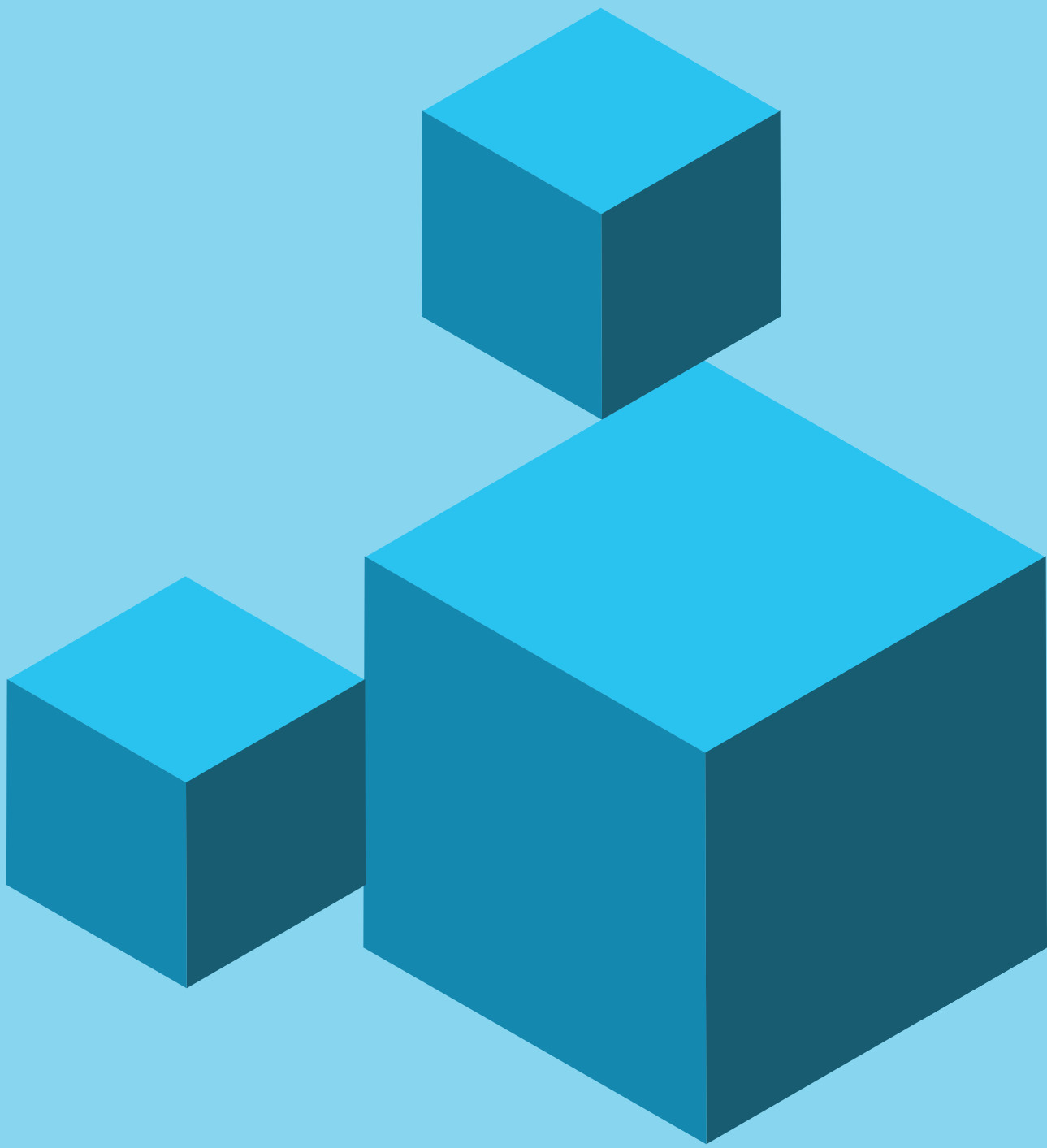
SIGURNA ŠKOLA U DIGITALNOM OKRUŽENJU

End Violence Against Children
THE FUND

Save the Children
100 YEARS

MEĐUNARODNI FORUM SOLIDARNOSTI - EMMAUS
BOSNA I HERCEGOVINA

unicef
za svako dijete



Dijete i škola u digitalnom okruženju

Prateći tehnološki razvoj, sve škole u Bosni i Hercegovini (BiH) imaju tendenciju unapređenja informatičkih kapaciteta, uključujući čuvanje, obradu i korištenje podataka o djeci i zaposlenima. Stoga se opravdanim smatra raspravljati i istraživati o sigurnosti školskih servera.

Umreženi računari, ukoliko nisu dio dobro konfigurisane mreže u smislu sigurnosti, izuzetno su ranjivi na razne vrste računarskih napada. Podaci dobijeni tehnologijom Intelligent Security Graph[1] pokazuju da je potrebno samo 24 do 48 sati da se zlonamjerni software proširi kompletnom mrežom nakon kompromitacije samo jednog računara, a prosječno vrijeme do otkrivanja kompromitovanosti je čak 150 dana.

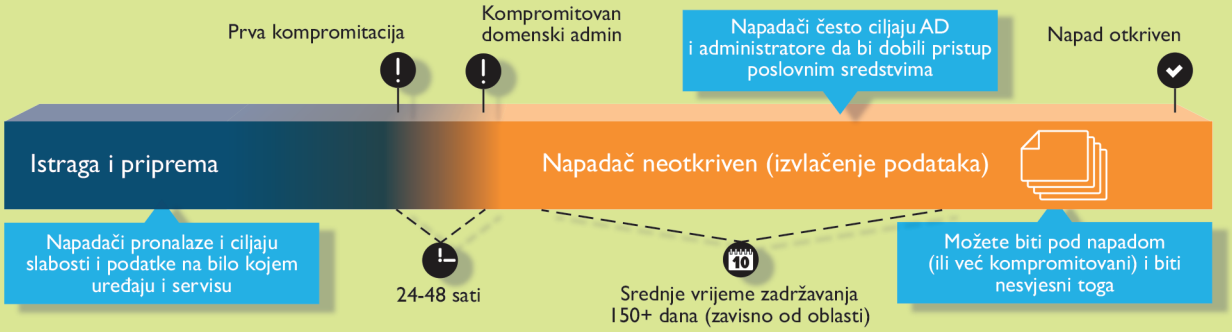
Većina škola u BiH ne koristi nikakvu vrstu serverske infrastrukture[2], bilo da se radi o vlastitim serverima ili javnom, privatnom ili hibridnom oblaku. To ukazuje da postoji velika količina heterogenih podataka „razbacanih" na pojedinačnim računarima koje koristi školska administracija, pa vrlo lako i dugoročno mogu postati dostupni neautorizovanim korisnicima i iskorišteni za nelegalne aktivnosti. Iako je većina nadležnih ministarstava u BiH osigurala da se elektronski dnevnik i slične baze ličnih podataka učenika čuvaju u infrastrukturi koja je na neki način povezana sa vladinom infrastrukturom (npr. EMIS), postoji značajna količina bitne dokumentacije, koja uključuje i lične podatke, a za koju nije predviđena nikakva sistematizacija i zaštita.

Kako lični podaci koje škola prikuplja, čuva i obrađuje, uključuju i telefonske brojeve i adrese stanovanja, jasno je da je dostupnost ovakvih podataka veoma opasna.

[1]Tehnologija kompanije Microsoft koja prikuplja veliku količinu podataka o sigurnosti sa računara pokretanih Windows 10 operativnim sistemom. Više na: https://www.microsoft.com/en-us/security/operations/intelligence

[2]Rezultati iz istraživanja sigurnosti školskih servera u okviru projekta „Prevencija i rad na sprečavanju seksualnog iskorištavanja i zlostavljanja djece u digitalnom okruženju u Bosni i Hercegovini" koji provode organizacije Save the Children, UNICEF i EMMAUS

Vremenska linija napada



Zlonamjerne osobe bi ove podatke mogle iskoristiti, između ostalog, za lažno predstavljanje, kao i za direktan pristup potencijalnoj žrtvi. Upravo to često i biva uvodni dio kod slučajeva seksualnog iskorištavanja i zlostavljanja djece u digitalnom okruženju. Ranjivost djece u BiH je potvrđena rezultatima Studije o navikama i ponašanju djece na internetu, iz koje se izdvajaju sljedeći podaci:[3]

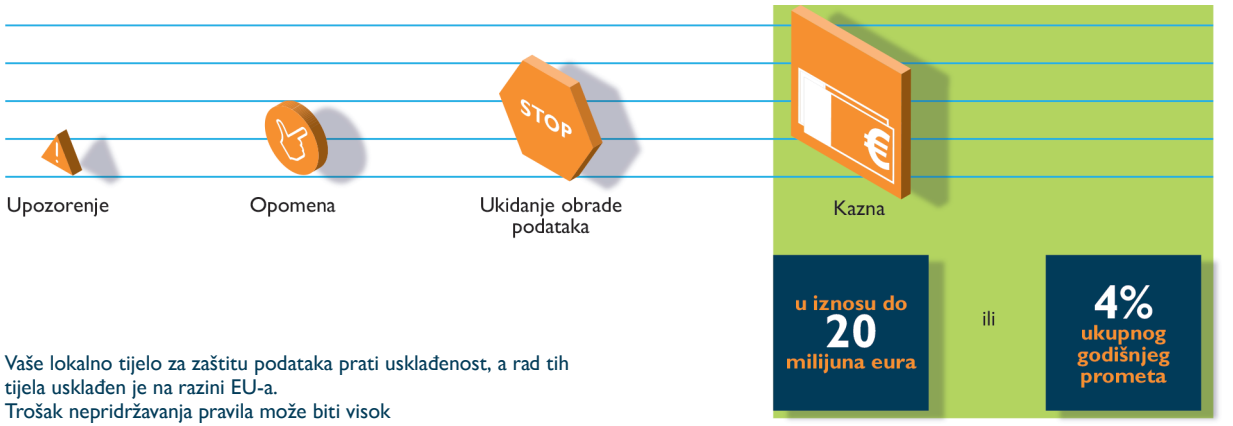
- 48,5% djece kaže da su dobijali poruke od nepoznatih lica;
- 43,3% je prihvatalo nepoznata lica za prijatelja na nekoj od društvenih mreža;
- 27,8 % djece se dopisivalo sa nepoznatima;
- 11,4% djece je pristalo da se sastane sa nepoznatim licima koja su upoznali putem interneta.

Posebno treba napomenuti da je od 2018. godine na snagu stupila Opšta evropska regulativa o zaštiti podataka[4] koja se odnosi i na bilo koji podatak evropskih građana i izvan Evropske unije, te predviđa značajne finansijske kazne ukoliko podaci nisu obrađivani u skladu sa ovom regulativom. Ilustracija 2. prikazuje infografiku o tipovima sankcija u slučaju kršenja ove regulative. Pored činjenice da BiH teži ka ulasku u Evropsku uniju, sasvim je izvjesno da među učenicima u BiH ima onih koji posjeduju državljanstvo neke od zemalja članica Evropske unije, pa se spomenuta regulativa već može primijeniti u nekim slučajevima i nekim školama. Tako, sigurnost podataka u školama i sigurnost školskih servera postaje jedan od prioriteta informacione sigurnosti školskog sistema.

[3] Muratbegović i Vujović, Ponašanje i navike djece na internetu: stavovi djece, roditelja i nastavnika informatike, 2016.

[4] Više detalja na zvaničnom portalu Evropske komisije: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_hr

Trošak neusklađenosti



Vaše lokalno tijelo za zaštitu podataka prati usklađenost, a rad tih tijela usklađen je na razini EU-a.
Trošak nepridržavanja pravila može biti visok

Rizici po informacionu sigurnost i posljedice njihove manifestacije

„CURENJE“ PODATAKA

Curenje podataka može biti namjerno ili nenamjerno dijeljenje i/ili objavljivanje povjerljivih informacija. Nesprečavanje ovakvog incidenta može dovesti do ozbiljnih pravnih posljedica, pogotovo ako su podaci barem dijelom obuhvaćeni GDPR-om.

RANSOMWARE NAPAD

Radi se o zlonamjernoj enkripciji podataka izazvanoj zlonamjernim softwareom na pojedinim računarima ili čak u čitavoj mreži u kojoj se nalazi zaraženi računar. Podacima se ne može prići dok se ne uplati određeni novčani iznos, a podatke je u većini slučajeva nemoguće otkriti.

NEZAKLJUČANI RAČUNARI

Ukoliko ne poštujemo pravilo da računar uvijek mora biti zaključan kada se na njemu ne radi, ostavljamo mogućnost da zlonamjerne osobe dobiju djelomični ili potpuni pristup raznim vrstama osjetljivih podataka.

ZAJEDNIČKE LOZINKE

Korištenje zajedničkih lozinki ili jedne lozinke za više sistema i aplikacija je značajan sigurnosni rizik.

DATOTEKE U MAILU

Kako je elektronska pošta veoma bitan dio poslovne i privatne komunikacije, velika je vjerovatnoća da korisnik dobije i zlonamjernu datoteku kao dodatak poruci. Bitno je da su korisnici svjesni opasnosti te da su uspostavljeni efikasni sistemi za kontrolu elektronske pošte.

IZMJENJIVI MEDIJI I USB MEMORIJA

Prenosivi mediji su uobičajeni način prenosa veće količine podataka. Rizici su brojni, uključujući gubitak podataka, malware, gubljenje medija, što može dovesti do gubljenja ugleda i povjerenja. Pronađena USB memorija može sadržavati zlonamjeran software te neoprezno korištenje takvih uređaja može biti veoma rizično.

DRUŠTVENI INŽENJERING

Društveni inženjering je upotreba obmane u cilju manipulacije pojedinaca kako bi otkrili povjerljive ili lične podatke te podatke koji se mogu iskoristiti za zaobilaženje sigurnosnih mjera.

SPYWARE

Spyware i malware su vrste zlonamjernog softwarea koji omogućavaju pristup skrivenim informacijama o aktivnostima određenog korisnika i računara te slanje tih podataka neovlaštenim osobama.

PHISHING

Phishing je slanje lažnih poruka e-pošte u kojima naizgled stvarne kompanije i institucije traže unos ličnih i autentifikacijskih podataka.

„ČOVJEK U SREDINI“ NAPADI

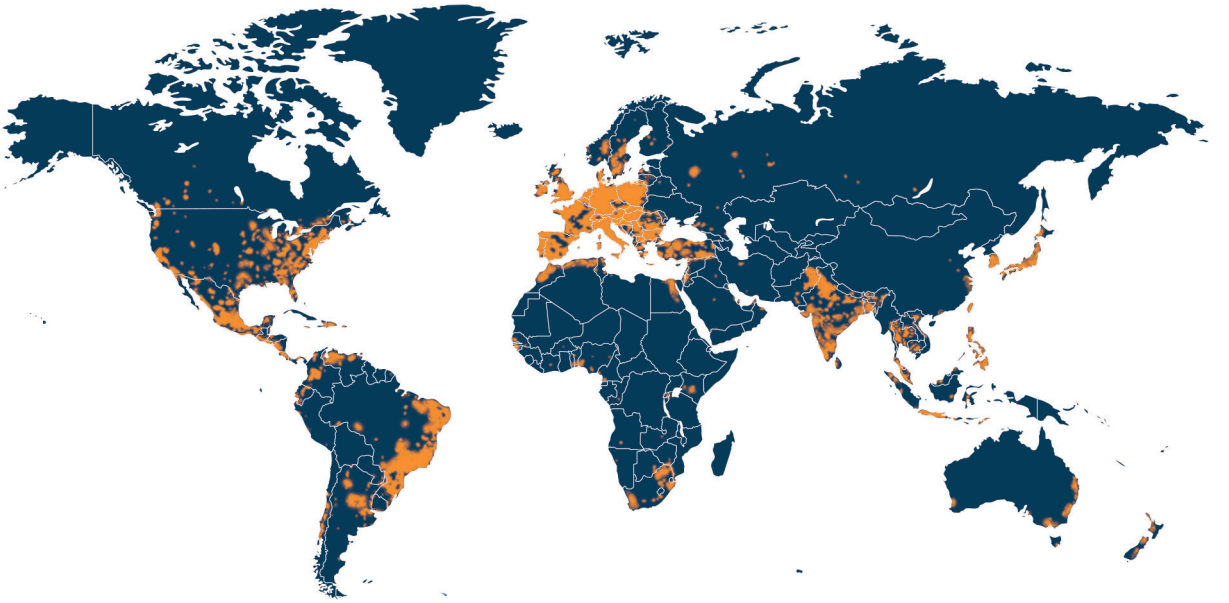
Ukoliko žične i bežične mreže nisu ispravno i profesionalno konfigurisane, moguće je da se neželjene osobe uključe u takvu mrežu i nadgledaju sav promet otkrivajući na taj način osjetljive informacije i pristupne podatke.

Savremena društva i ekonomije su u konstantnom procesu digitalne transformacije, te su navedeni rizici samo dio prijetnji sigurnosti informacija u digitalnom okruženju. Prema Microsoftovom Izvještaju o sigurnosti iz marta 2018. godine[5], botnet mreža[6] je uključivala 1214 domena i IP adresa sa 464 različita botnet sistema i više od 80 različitih malware porodica. Jedna od najzastupljenijih botnet mreža je bila Gamarue mreža sa više od 23 miliona IP adresa (na Ilustraciji 3. možemo vidjeti geografsku rasprostranjenost te mreže, a na Ilustraciji 4. broj uređaja u mreži).

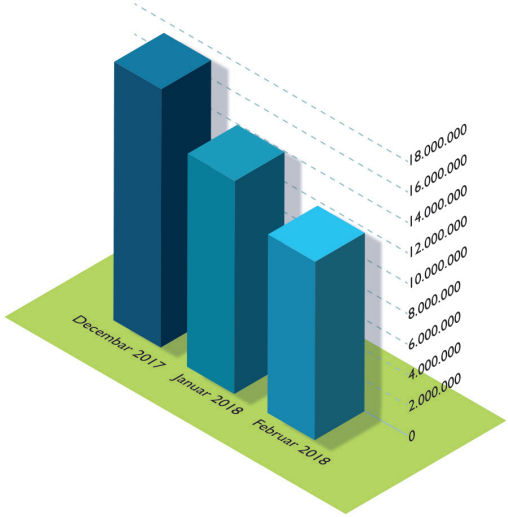
[5] Više na https://cloudblogs.microsoft.com/microsoftsecure/2018/03/15/microsoft-security-intelligence-report-volume-23-is-now-available/

[6] Botnet mreže su mreže zaraženih računara nad kojima kontrolu imaju korisnici zlonamjernog softwarea koji se nalazi na tim računarima te se koriste za razne vrste napada. Vlasnici i korisnici tih računara najčešće nisu ni svjesni da je računar kompromitovan.

Ilustracija 3. Telemetrija Gamarue mreže (decembar 2017. – januar 2018.)



Ilustracija 4. Broj uređaja u Gamarue mreži prije i poslije otkrivanja (januar 2018)



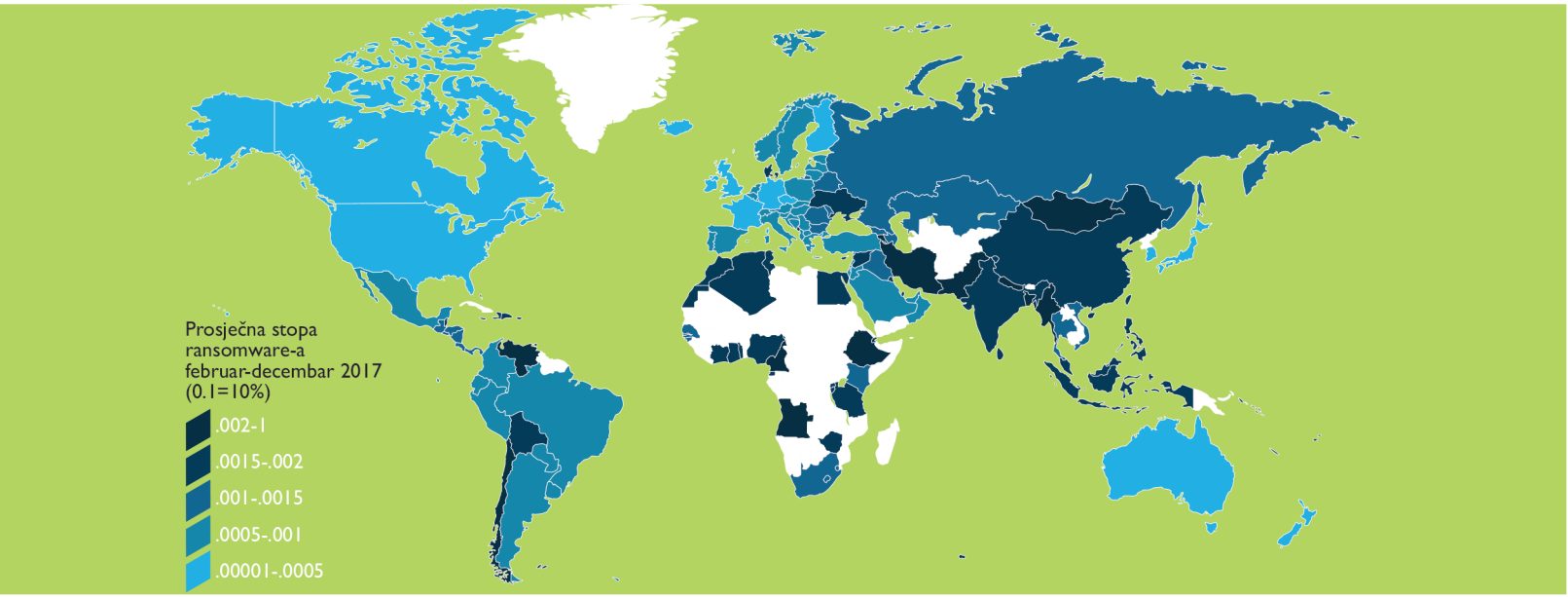
Najzastupljeniji ransomware napadi su bili tipa: WannaCrypt[7], Petya[8] i BadRabit[9]. Na Ilustraciji 5. je prikazana zastupljenost ransomware napada u periodu februar – decembar 2017. godine.

[7] Više detalja na: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/WannaCrypt

[8] Detaljnije na: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Petya.B

[9] Opširnije na: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Tibbar.A

Ilustracija 5. Rasprostranjenost ramsonwarea



Više detalja o vrstama i zastupljenosti raznih napada i sigurnosnih rizika dostupno je u Microsoft Izvještaju i Cisco godišnjem izvještaju o sigurnosti[10], a izdvojeni podaci su prikazani na Ilustraciji 6.

[10] Kompletan izvještaj: https://www.cisco.com/c/en/us/products/security/security-reports.html

Ilustracija 6. Izdvojeni podaci iz Cisco Anual Cybersecurity Report

PDF dokumenti su najčešća meta unutrašnjih prijetnji.

Jedan sumnjivi korisnik može imati veliki uticaj.

53%

53% korisnika koji se uspješno brane više od pola infrastrukture drže u oblaku.

Zašto? Jednostavno, bezbjednije je.

34%

34% profesionalaca za bezbjednost potpuno se oslanja na mašinsko učenje.

Jednostavnija i automatizovanija bezbjednost.

Mobilni uređaji su prioritet.

Prema ovom istraživanju najteže se štite.

milion

Nyetya je bila instalirana na više od milion računara

Često putem automatskih nadogradnji software-a.

Korisnici preferiraju provjerena rješenja.

72% koristi provjerena rješenja za zaštitu.

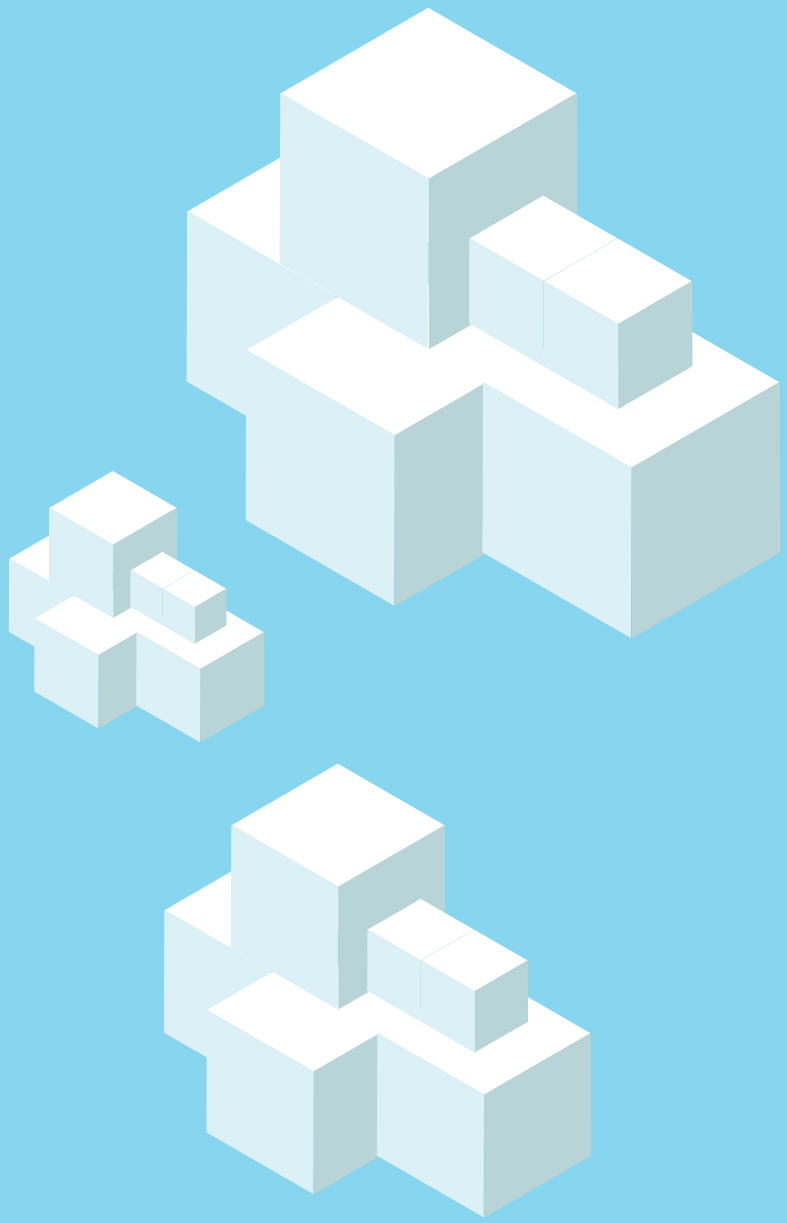
3

Šta škole mogu
i treba da preduzmu?

Sa ciljem zaštite sigurnosti podataka djece, a time i prevencije kibernetičkog kriminala, škole mogu da preduzmu dvije vrste mjera, i to: (a) mjere edukacije, i (b) mjere tehničke zaštite.

a. Mjere edukacije:

- provesti edukacije za sve nastavnike i stručne radnike škole, sa ciljem podizanja svijesti i znanja o informacionoj sigurnosti, uključujući kreiranje i isticanje edukativnih materijala;
- osigurati odgovarajuće obuke za školsko osoblje koje direktno radi na prikupljanju, čuvanju, obradi ličnih podataka djece, odnosno za osobe koje imaju pristup bazama podataka o djeci i zaposlenima;
- podržati provođenje edukativnih radionica sa roditeljima i djecom, uključujući kreiranje i isticanje edukativnih materijala;
- upoznati se s načinom kreiranja procedura o prikupljanju, obradi i korištenju ličnih podataka, te ih kreirati;
- po potrebi, uspostaviti saradnju sa nadležnim institucijama koje mogu pružiti podršku u vezi sa zaštitom ličnih podataka.



b. Mjere tehničke zaštite:

Osnovne karakteristike i funkcionalnosti dobro zaštićenih servera i računarskih mrežnih sistema

KONTROLA PRIJAVE

Lozinke treba da budu minimalne dužine 8 karaktera sa kombinacijom velikih i malih slova i barem jednim brojem i specijalnim karakterom

Lozinke se moraju redovno mijenjati

Ukoliko je to moguće, upotrebljavati dvofaktorsku autentifikaciju

SIGURNO POHRANJENI IDENTITETI

Lozinke moraju biti hashirane[11] prije pohrane u direktorijsku bazu

Korisnici i grupe koje više nisu potrebne i ne upotrebljavaju se treba izbrisati

Prije pohrane bilo kakvih podataka obaviti antivirusnu provjeru

OSVJEŽENI I AŽURIRANI OPERATIVNI SISTEMI I APLIKACIJE

Redovnim održavanjem sistema kroz sistem nadogradnji i zakrpa osigurava se ne samo bezbjedan sistem nego omogućava i optimizovaniji, pouzdaniji i brži rad

KVALITETAN I POUZDAN SISTEM VATROZIDA

Vatrozid omogućava dodatnu nadogradnju sigurnosnih karakteristika koje postoje u operativnom sistemu.

AUTENTIFIKACIJA SSH[12] KLJUČEVIMA

SSH ključevi su dobar alternativni način prijave u odnosu na kombinaciju korisničko ime i lozinka- Kriptografski ključevi sadrže značajno više bitova podataka nego lozinke

UPOTREBA VPN[13] -a KAD GOD JE TO MOGUĆE

ENKRIPCIJA PODATAKA

Enkripcija omogućava da samo osobe sa autorizacijom mogu pristupiti podacima i izvršiti dekripciju

INSTALIRANJE POUZDANOG I PROVJERENOG SOFTWAREA

Instaliranje aplikacija izdatih od provjerenih kompanija prevenira značajan dio sigurnosnih rizika

REDOVNO PRAĆENJE SLABOSTI

Rano saznanje o slabostima sistema omogućava pravovremenu implementaciju protivmjera

BACKUP PODATAKA

Uraditi backup enkriptovanih podataka koji sadrže osjetljive informacije uz korištenje dodatne lozinke ukoliko nam sistem to omogućava.

ANGAŽMAN IT PROFESIONALCA

NEOPHODNO JE DA O SIGURNOSTI PODATAKA BRINU PROFESIONALCI. DOBRO RJEŠENJE JE I VANJSKI SARADNIK UKOLIKO NEMA MOGUĆNOSTI STALNOG ZAPOSLENJA.

[11] Procedura čuvanja podataka u šifrovanom obliku. Tako bi npr. riječ „lozinka“ šifrovana MD5 algoritmom bila pohranjena kao „8AA87050051EFE26091A13DBFDF901C6“

[12] SSH ključevi su dodatak kombinaciji korisničkog imena i lozinke i koriste se za uspostavljanje sigurne i šifrovane veze između dva računara, obično korisničkog računara i servera

[13] Virtuelna privatna mreža kreirana korištenjem interneta. Iako se komunikacija odvija putem javne internet mreže, između računara je uspostavljena sigurna i privatna kopija lokalne mreže.

Save the Children za sjeverozapadni Balkan
Ljubljanska 16, Sarajevo, Bosna i Hercegovina

Tel +387 (0) 33 290 671, Fax +387 (0) 33 290 675 |
info.nwbalkans@savethechildren.org

https://nwb.savethechildren.net
savethechildrennwb
savethechildrennwb
scnwb
SavethechildrenNWB

Zajedno možemo učiniti više. Šta misliš o našem radu?
reci-nam@savethechildren.org

Ova brošura je izrađena u okviru projekta "Zaustaviti nasilje nad djecom: Prevencija i rad na spriječavanju seksualnog iskorištavanja i zlostavljanja djece u digitalnom okruženju u Bosni i Hercegovini", čiju su realizaciju podržali Global Fund to End Violence Against Children i UNICEF.