Email bezbednost

Upravljana usluga prevencije od zloupotreba i napada putem email kanala

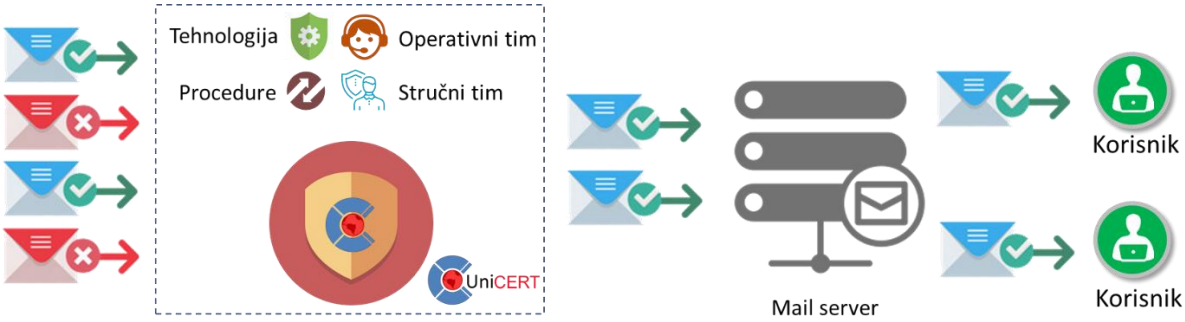
Email predstavlja najrasprostranjeniji a pri tom najranjiviji kanal komunikacije na internetu (91% sajber napada upravo počinje preko emaila), zahvaljujući masovnoj upotrebi i jednostavnim mogućnostima zloupotrebe (*protokol za razmenu email saobraćaja SMTP koji je i danas u upotrebi nastao je 1982. godine, a revidiran 2008. nije predviđao odgovarajuće sigurnosne koncepte*). Korisnici su konstantno izloženi pretnjama kao što su spam-ovi, virusi i napredni oblici pretnji, i njihov obim se stalno povećava. Najveći broj pretnji upravo stiže kroz email kanal u formi zlonamernih aplikacija kao priloga (attachment), malicioznih linkova ili lažnog predstavljanja sa namerom ostvarivanja kriminalnih ciljeva kao što su dalja infiltracija u informacioni sistem, krađa podataka, kodiranje podataka uz traženje otkupa (ransomware), iznuda novčanih uplata. Tradicionalni anti-virus i anti-spam mehanizmi su dobri u sprečavanju jednostavnih, već poznatih oblika masovnih napada ali ne mogu da odgovore današnjim oblicima pretnji koji lako zaobilaze ove sisteme zaštite. Email zato i dalje ostaje primarni kanal naprednih oblika napada (npr. ransomware, iznude) pošto lako dolazi do mete uz veoma dobru mogućnost prilagođavanja kako bi zaobišao mehanizme zaštite i prevario metu.

Opis usluge

Usluga Email bezbednosti predstavlja najefikasniji vid zaštite od svih oblika savremenih pretnji koje su karakteristične za email kanal. Kroz uslugu se vrši detekcija i prevencija od svih oblika napada od jednostavnijih do složenih, što podrazumeva odstranjivanje zlonamernog sadržaja hirurškom preciznošću iz email komunikacije. Bilo da se radi o zlonamernom sadržaju poslatom kao prilog ili link u email-u, ili da se radi o lažnom predstavljanju, usluga vrši „čišćenje“ email saobraćaja od ovih pretnji kako bi do korisnika stigla samo legitimna komunikacija.

Usluga se jednostavno implementira preusmeravanjem DNS zapisa za mail server (MX zapisa) na adrese platforme za zaštitu. Preusmeravanjem saobraćaja servisna platforma postaje front za prijem email komunikacije, vrši analizu poruka i u slučaju da je detektovan zlonameran sadržaj, vrši se odstranjivanje tog sadržaja ili se poruka blokira uz odgovarajuće obaveštenje. Platforma prosleđuje dalje „očišćenu“ i legitimnu komunikaciju prema email serveru korisnika.

Klijent ima uvid u sve informacije vezane za uslugu kroz korisnički portal. Svi događaji vezani za prevenciju i detekciju zlonamernog sadržaja su dostupni kroz portal. Slučajevi usmerenih napada na organizaciju se tretiraju kao kritični incidenti i u tom slučaju se vrši automatsko otvaranje servisnog slučaja u tiketing sistemu i u zavisnosti od prioriteta vrši se obaveštavanje korisnika (kod prioritetnog incidenta poziva se ovlašćena osoba klijenta). Sva komunikacija između korisnika beleži se kroz tiketing sistem koji istovremeno prati parametre servisnog nivoa (SLA). Korisnik dobija i mesečne izveštaje koje uključuju rad servisa i statistike vezane za incidente.



Najčešća pitanja

Zašto email bezbednost ?

Kako je objašnjeno u uvodu, email kanal je jedan od najbitnijih kanala komunikacije, bez kojeg ni jedna organizacija ne može da obavlja poslovanje. Sa druge strane email kanal po svom konceptu nije bezbedan, pošto svako može da pošalje email, a da ne možemo biti sigurni u identitet pošiljaoca. To sve zajedno otvara velike mogućnosti zloupotrebe, što po najrazličitijim načina zloupotrebe, što po masovnosti. Statistike pokazuju da 91% napada započinje upravo kroz mail kanal, dok 73% zlonamernog sadržaja se prenese putem maila. Osnovni mehanizmi na mail serverima kao što su anti-virus i anti-spam ne mogu da pruže zaštitu od današnjih pretnji i zlonameran sadržaj u obliku priloga (attachment), malicioznih linkova ili lažnog predstavljanja prolazi neprimećen do primaoca i dolazi do dalje infiltracije, krađe podataka, kodiranje podataka uz traženje otkupa (ransomware) ili iznuda novčanih uplata.

Ono što nije statistika već činjenica da je **samo <u>jedan</u> uspešan napad dovoljan da dođe do ozbiljnih gubitaka**.

Koje su tipične pretnje i napadi vezani za email?

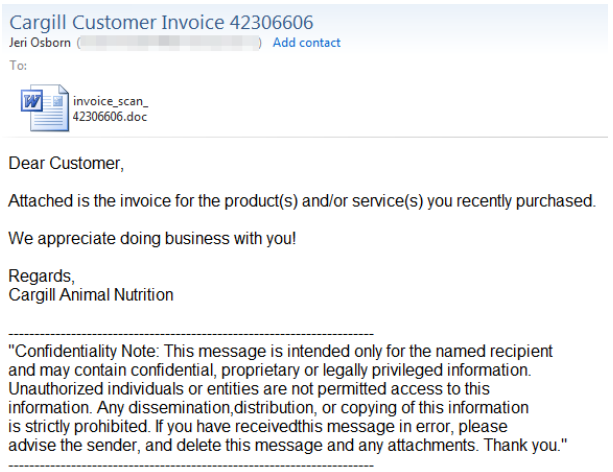
Zajednička karakteristika svih pretnji vezanih za email kanal je da su poruke „maskirane“ kao da su došle od poznatog pošiljaoca i/ili imaju lažni sadržaj koji može da probudi radoznalost primaoca. To su najčešće poruke koje izgledaju kao da su došle od neke poznate organizacije (banke, google-a, facebook-a…), neke poznate osobe ili čak i uređaja (npr. skener). Takve poruke izgledaju (skoro) u potpunosti isto kao i originalni i legitimni mailovi (logo, dizajn…)

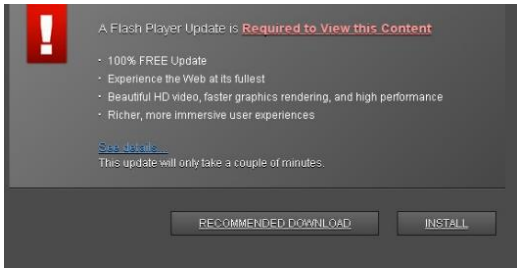
Pretnje i napade možemo podeliti u dve grupe:

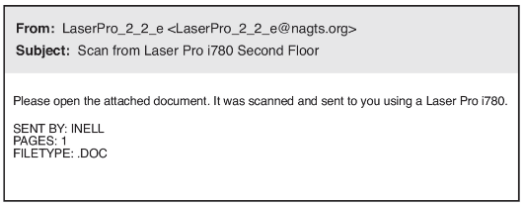
1. Emailovi koji sadrže ili upućuju na zlonamerni programe čijim izvršavanjem se inficira računar što dovodi do negativnih posledica. Svojim sadržajem navode primaoca:
    a. da otvori fajl koji se nalazi u prilogu - npr. tvrdi se da je fajlu u prilogu račun ili neki drugi sadržaj koji može da izazove interesovanje primaoca. Ovi fajlovi sadrže zlonamerne programe koji se aktiviraju otvaranjem i dovode do ozbiljnih posledica – zaključavanje/kodiranje fajlova uz

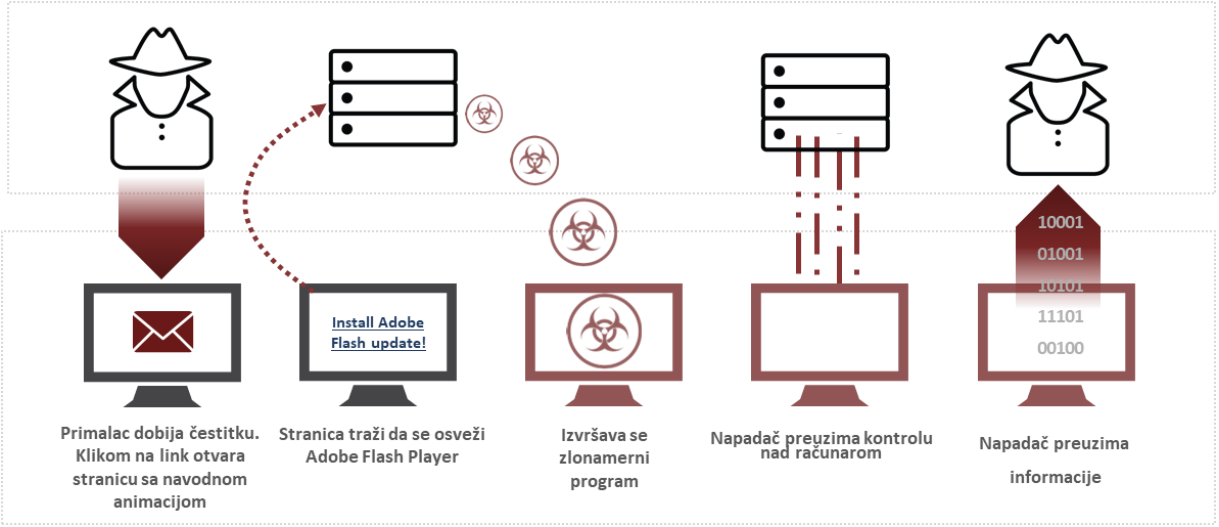
najčešće traženje otkupa (ransomware) ili prikupljanje lozinki korisnika, preuzimanje dalje kontrole nad radnom stanicom, dalja infiltracija u informacioni sistem itd.

b. da klikne na neki link - npr. u okviru praznične čestitke vidno stoji link koji treba da otvori animiranu verziju čestitke. Klikom na link, otvara se stranica koja traži od korisnika da instalira npr. Adobe Flash player kako bi se mogla pogledati animirana čestitka. Klikom na instalaciju izvršava se program koji dovodi do istih posledica kao u slučaju otvaranja fajla u prilogu (ransomware itd.).



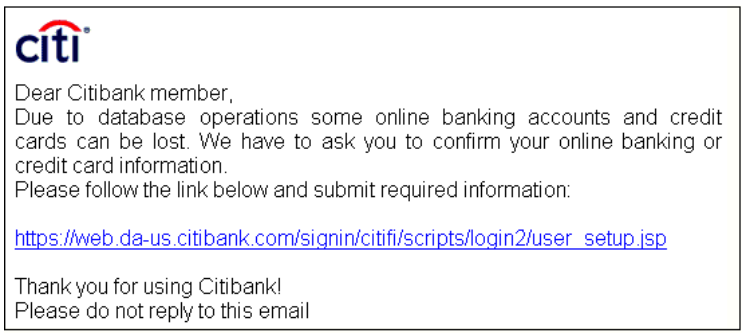






2. Emailovi koji ne sadrže eksplicitan zlonameran program koji se može izvršiti na računaru već svojim sadržajem navode primaoca da preduzme neke korake sa negativnim posledicama. Najčešće se srećemo sa dva oblika ovakvih napada:
   a. Krađa lozinke - npr. u poruci se tvrdi se da je istekla lozinka za pristup ebanking-u, i traži se da primalac klikne na link da bi promenio lozinku. Klikom na link otvara se stanica koja je skoro ista kao i legitimna bančina, ali se najčešće traži da se upiše i sadašnja lozinka. Na taj način se dolazi do lozinke, pomoću koje se vrše kasnije zloupotrebe.
   b. Kompromitacija poslovnog maila (BEC - Business Email Compromise / CEO scam). Tipičan scenario izgleda ovako: Napadač posle istraživanja kompanije i ključnih osoba, uputi mail npr. nekoj osobi u finansijskoj službi koja ima ingerencije, da po hitnom postupku uplati određeni iznos na određeni broj računa, a pri tom se izdaje za najčešće za direktora ili vlasnika. Primalac

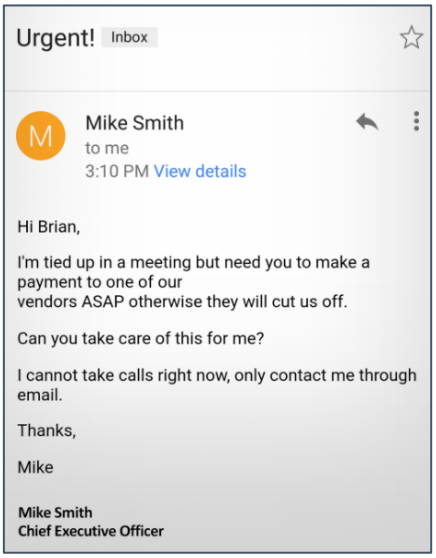
tj. žrtva na osnovu sadržaja ili izgleda maila, realizuje ovaj zahtev sa ubeđenjem da je poruka zaista došla od legitimnog pošiljaoca, direktora ili vlasnika. Jedno od medijski zabeleženih prevara ovakvog tipa u Republici Srbiji dogodio se 2017., gde je žrtva bila Narodna Banka Srbije.


citi

Dear Citibank member,
Due to database operations some online banking accounts and credit cards can be lost. We have to ask you to confirm your online banking or credit card information.
Please follow the link below and submit required information:

https://web.da-us.citibank.com/signin/citifi/scripts/login2/user_setup.jsp

Thank you for using Citibank!
Please do not reply to this email


Urgent! Inbox

Mike Smith
to me
3:10 PM View details

Hi Brian,

I'm tied up in a meeting but need you to make a payment to one of our
vendors ASAP otherwise they will cut us off.

Can you take care of this for me?

I cannot take calls right now, only contact me through email.

Thanks,

Mike

Mike Smith
Chief Executive Officer

Zašto anti-virus i anti-spam nisu dovoljni i kako detektovati i sprečiti pretnje?

Anti-spam mehanizmi vrše filtriranje email poruka sa ciljem odbacivanja neželjenih reklamnih i zlonamernih poruka. Anti-spam je veoma koristan u odbacivanju masovnih reklamnih poruka, pošto može da prepozna ključne reči i obrasce i na taj način oslobodi korisnika velike količine neželjenih poruka. Sa druge strane anti-spam ne može da prepozna zlonamerni sadržaj niti lažno predstavljanje ili kompromitaciju poslovnog maila (BEC - Business Email Compromise).

Antivirusi predstavljaju odbranu iz prošlog vremena. Antivirus programi se baziraju na zaštiti isključivo od poznatih oblika malvera (virusa) – malvera koji je već ranije prepoznat negde, i njegov „otisak“ ubačen u bazu. Samo u prošloj 2017 godini se pojavilo više od 120 miliona novih malvera što je više od 300.000 novih malvera dnevno. Po statistici se 80% zlonamernih programa pojavljuje samo jednom, dok je 68% zlonamernih programa jedinstveno za napad na jednu organizaciju. Antivirusi ne mogu da detektuju ovakve zlonamerne sadržaje, koji danas predstavljaju najzastupljeniju pretnju.

Efikasna detekcija i prevencija treba da predstavlja kombinaciju različitih mehanizama među kojima je najvažniji prepoznavanje zlonamernog sadržaja po ponašanju, da bi se omogućila detekcija ranije nepoznatih oblika napada kao i „mutacija“ virusa (isti virus, sa istim ponašanjem ali sa drugačijim sadržajem koji može u svakoj instanci da bude drugačiji). Potrebna je i kompletna analiza email poruka što uz analizu fajlova u prilogu treba da uključi i analizu sadržaja na koji linkovi u poruci upućuju. Takođe, potrebno je primeniti i odgovarajuće mehanizme za detekciju kompromitacije poslovnog maila, kako bi se zaokružila zaštita od svih relevantnih pretnji.

Kako usluga email bezbednosti odgovora na ova pitanja

Zašto email bezbednost ?

Usluga se fokusira na zaštitu od pretnji koji su vezani za email. Postoje i drugi bezbednosni izazovi koji se moraju rešavati drugim pristupom (zaštita od curenja informacija, zaštita infrastrukture od mrežnog ili aplikativnog napada itd.), ali zbog činjenice da email kanal ima najzastupljeniju ulogu u sajber napadima, ovaj vid zaštite može da eliminiše veliki procenat bezbednosnih rizika.

Koje su tipične pretnje i napadi vezani za email?

Usluga email bezbednosti može uspešno da odgovori tj. da zaštiti sistem od najčešćih oblika pretnji što podrazumeva i kvalitetnu detekciju sa zanemarljivim udelom lažnih pozitiva (false-positive). Štiti od svih oblika pretnji:

- Detektuje i blokira zlonamerni sadržaj u poruci i prilogu
- Detektuje i blokira zlonamerni sadržaj koji se potencijalno aktivira klikom na link iz maila
- Detektuje i blokira poruke koje navode na krađu lozinki
- Detektuje i blokira prevare sa kompromitacijom poslovnog maila

Zašto anti-virus i anti-spam nisu dovoljni i kako detektovati i sprečiti pretnje?

Usluga email bezbednosti kombinuje različite napredne mehanizme u detekciji i prevenciji pretnji koji zajedno doprinose eliminacije visokog procenta rizika vezanih za ovaj kanal. Primarna detekcija se vrši simuliranom analizom ponašanja svih relevantnih elemenata poruke u bezbednom virtuelnom okruženju. Ova simulacija podrazumeva izvršavanje dokumenta iz priloga veoma slično kao što bi primalac to uradio na svom računaru. Virtuelno izvršno okruženje može da detektuje maliciozno ponašanje i blokira poruku ili ukloni dodatak pre nego što poruka stigne do korisnika. Takođe, na isti način se ispituje rizičnost linkova u poruci, virtuelno okruženje pokreće i analizira ponašanje sadržaja na koji linkovi upućuju i uklanja rizične linkove ili blokira poruku ukoliko postoji pretnja. Virtuelno okruženje analizira sadržaj na različitim okruženjima, i različitim verzijama aplikacija i operativnih sistema kako bi detekcija bila još kvalitetnija. Posebni mehanizmi su odgovorni za kvalitetnu detekciju prevara bez prisustva zlonamernih programa u poruci (krađa lozinke i kompromitacija poslovnog maila)

Svi ovi mehanizmi su obezbeđeni tehnologijom vodećih kompanija u domenu sajber bezbednosti.

Pored tehnologije neizostavni su i ljudski resursi. Usluga obezbeđuje raspoloživost 24/7 operativnog tima, koji nadgleda sistem, analizira događaje i reaguje po potrebi.

Šta je prednost naših usluga ?

Trenutna implementacija
Implementacija u istom danu od trenutka aktivacije servisa. Jednostavno puštanje u rad, tehnologija, procedure i ljudi spremni za pružanje usluge.

Vodeće tehnologije
Tehnologije koje se koriste u sklopu usluge prestavljaju vodeća rešenja iz svojih oblasti, odabrana da pruže najviši kvalitet i najbolju mogućnost integracije sa ostalim elementima usluge.

Operativni centar 24/7
U sklopu usluge na raspolaganju je stalno dostupan 24/7 operativni tim u okviru savremenog sigurnosnog operativnog centra (SOC)

Ekspertski tim
Pored operativnog tima, stručni tim sa višegodišnjim iskustvom iz domena sajber bezbednosti može uspešno da odgovori na sve izazove !

Bezbednost
Kako je naša osnovna delatnost informaciona bezbednost, pobrinuli smo se da vaši podaci budu bezbedni. Cela infrastruktura kao i data centar je pod našom direktnom kontrolom na teritoriji Republike Srbije.

Isporuka usluge - SLA
Precizno definisan nivo servisa (SLA), sa odgovarajućim ključnim indikatorima performansi (KPI). Kroz servisni model *garantujemo* efikasnu isporuku usluge !

Jasna komunikacija
Portal servisa i ticketing omogućavaju sledljivost međusobne komunikacije bez obzira na kanal – automatika sistema, portal, email ili usmena komunikacija. Pored dostupne tehnologije, naš tim je uvek spreman da direktno pomogne !

Smanjenje troškova
Sve gore navedene prednosti doprinose krajnjem cilju – smanjenju troškova. Bezbedniji sistem znači manje gubitaka, a uz efikasnu isporuku usluge smanjuje se potreba za ulaganjem u (skuplje) interne resurse.

Dodatne informacije o usluzi

Ukoliko želite da dobijete dodatne informacije u vezi usluge možete da nas kontaktirate putem email-a services@unicom.systems ili na telefon 011 / 735-7150. Moguće je i zakazivanje sastanka sa prodajnim timom u okviru kog možemo odgovoriti na sva vaša pitanja, ukazati na sve detalje naše usluge i demonstrirati samu uslugu kroz realne situacije.