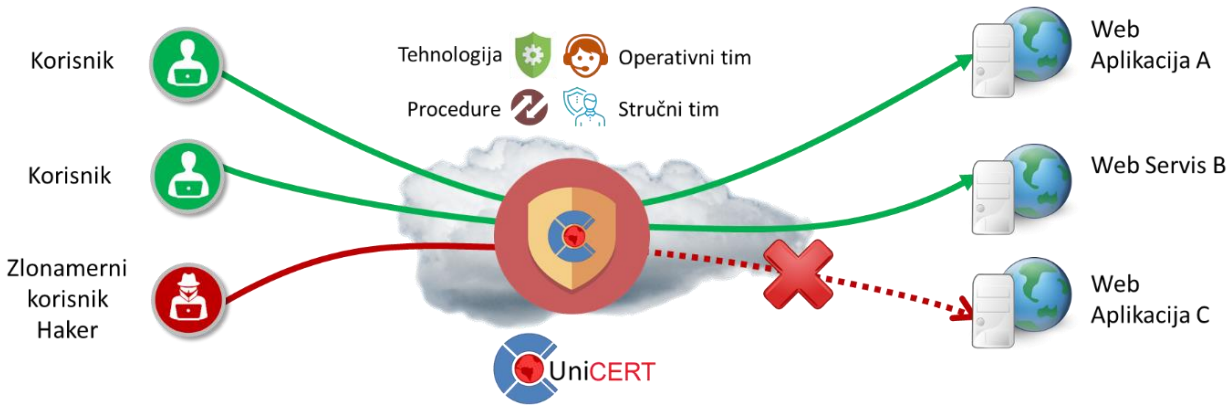
Zaštita aplikacija

Upravljana usluga sveobuhvatne zaštite web aplikacija

Opis usluge

Usluga zaštite aplikacija podrazumeva sveobuhvatnu zaštitu web aplikacija, servisa i povezane infrastrukture. Jedinstvena usluga pokriva zaštitu od najčešćih oblika pretnji – napada na infrastrukturu velikim brojem zlonamernih zahteva koji usporavaju i onemogućavaju rad (DoS/DDoS - Denial of Service / Distributed Denial of Service) kao i specifičnih napada na web infrastrukturu i aplikacije zloupotrebom ranjivosti sa ciljem infiltracije u sistem i kompromitacije informacija. Usluga zaštite aplikacija predstavlja kompletnu uslugu koja pored odgovarajuće tehnologije obezbeđuje i stalno dostupan tim eksperata koji predlaže i preuzima odgovarajuće korake u slučaju incidenta, u cilju eliminisanja negativnih posledica.

Usluga se jednostavno implementira preusmeravanjem DNS zapisa web i servisnih aplikacija na IP adrese platforme za zaštitu. Preusmeravanjem saobraćaja servisna platforma postaje front za sve korisnike aplikacija (kako za redovne korisnike, tako i za zlonamerne korisnike). Preusmeravanje saobraćaja se vrši na potpuno transparentan način, bez uticaja na korisničko iskustvo tj. potpuno nevidljivo za korisnike. Usluga zaštite aplikacija praktično vrši „čišćenje“, tako da do samih aplikacija stiže samo legitimni saobraćaj, eliminišući zlonamerni sadržaj.



Sistem vrši prevenciju od različitih oblika napada koji su tipični za aplikacije i infrastrukturu, detektuje mogući incident i po potrebi alarmira ekspertski tim. Ekspertski tim u slučaju incidenta momentalno reaguje, i u konsultaciji sa korisnikom preduzima odgovarajuće mere i daje dalje preporuke.

Klijent ima uvid u sve informacije vezane za uslugu kroz korisnički portal. Svi događaji vezani za prevenciju, detekciju i preduzete akcije su vidljivi kroz portal. Kritični incidenti vrše 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 i detaljne opise kritičnih incidenata i preduzetih mera.

Najčešća pitanja

Zašto je bitna zaštita aplikacija ?

Aplikacije predstavljaju najbitniji kanal interakcije kako unutar organizacije tako i sa klijentima i drugim licima sa kojima se vrši razmena informacija. One moraju biti izložene na internetu, dostupne za ceo svet. Samim tim predstavljaju vrlo ranjiv kanal koji se može na različite načine zloupotrebiti, stoga aplikacije zahtevaju specifične vidove zaštite od specifičnih rizika. Takođe, ova vrsta zaštite ne štiti samo aplikacije i odgovarajuću infrastrukturu već i ceo informacioni sistem, pošto se kroz iste može izvršiti infiltracija u druge delove sistema.

Koji su specifični rizici vezani za aplikacije ?

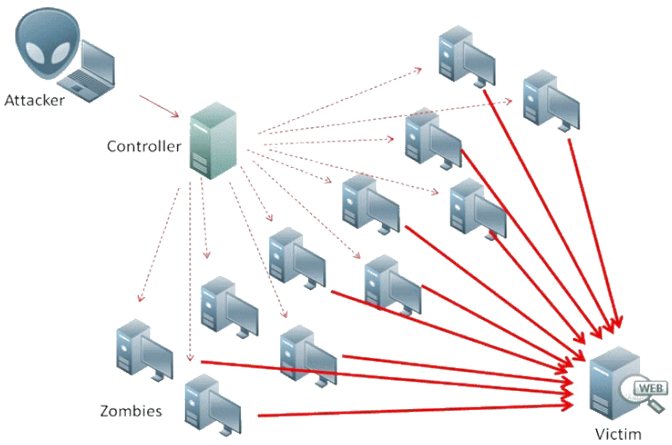
Specifične rizici vezani za aplikacije možemo generalno da podelimo u dve grupe:

1. Rizici koji su vezani za onemogućavanje rada aplikacije/infrastrukture/sistema – napadi na sistem koji dovode do otežanog ili potpunog sprečavanja rada aplikacije ili sistema velikim brojem zlonamernih zahteva i zahtevima koji koriste slabosti aplikacije ili protokola. Ove napade zovemo DoS/DDoS (Denial of Service / Distributed Denial of Service) napadima.
2. Rizici koji su vezani za kompromitaciju sistema – napadi na ranjivosti aplikacija ili infrastrukture sa ciljem infiltracije u sistem, krađe podataka, brisanja podataka, *defacement* - promena aplikacije/web stranice sa ciljem narušavanja ugleda (npr. stavljanje zastave neprijateljske zemlje na sajt državnih organa itd.)

Navedeni rizici ne mogu da se spreče tradicionalnim alatima kao što su fajervol (firewall) ili IPS (Intrusion Prevention System) već zahtevaju specifičnu infrastrukturu i tehnologiju koja ciljano štiti od navedenih tipova napada.

Šta je DDoS napad i koliki rizik predstavlja ?

DDoS napadi predstavljaju kontrolisan napad generisanjem zlonamernog sadržaja sa nekoliko desetina do nekoliko stotina hiljada uređaja/računara fokusiran na jedan sistem kao žrtvu. Uređaji tj. računari koji učestvuju u napadu, koji generišu zlonameran sadržaj predstavljaju zloupotrebljene sisteme - IoT uređaji, mrežni uređaji, serveri pa čak i računari na kojima radimo (bez svesti da upravo nevoljno učestvujemo u napadu) i kontrolisani su od strane napadača. Na ovaj način moguće je kreirati ogromnu količinu saobraćaja koji parališe žrtveni sistem.



Motivi za DDoS napade su različiti – od političkih do komercijalnih, česte su iznude, koje se sprovode sa istom namerom kao ransomveri, npr. napadne se žrtva pa se ucenjuje i uslovljava zaustavljanje napada za određenu finansijsku nadoknadu. DDoS napadi mogu da posluže i kao obmana, da prikriju pravi napad čiji je cilj dublja kompromitacija sistema.

Trendovi pokazuju da su DDoS napadi sve češći, sofisticiraniji i prouzrokuju sve veće i veće gubitke. Gubici, kao posledica napada, mogu biti ogromni (2013. godine napravljena je studija koja predviđa dnevne gubitke

od 10 miliona eura za državu Srbiju ukoliko se njena infrastruktura izloži napadu). Sa druge strane, sprovođenje DDoS napada je jednostavno i jeftino. Postoje usluge na internetu za DDoS napade (koji su „zvanično“ namenjeni za stres test infrastrukture) čija cena se kreće od nekoliko desetina dolara. Zbog ove nesrazmere između mogućih gubitaka i pristupačnosti i verovatnoće napada možemo da damo slikovito poređenje da mali miš može da uplaši i otera velikog slona.

Koji su rizici vezani za kompromitaciju sistema kroz (web) aplikacije ?

Za funkcionalnost (web) aplikacija potrebni su različiti sistemi – mreža, serveri, operativni sistemi, aplikativni serveri, baze podataka, drugi servisi sa kojima se aplikacija integriše. Unija svih ovih elemenata kumulativno povećava rizik sumiranjem svih specifičnih ranjivosti delova sistema – serveri imaju svoje specifične ranjivosti, aplikativni serveri, softverske platforme i naročito same aplikacije u smislu nedovoljne svesti o bezbednosti kod izrade aplikacija. Dodatno se rizik povećava time što aplikacije moraju biti izložene na internetu i dostupne svojim korisnicima.

Najčešće zloupotrebe proizilaze iz ranjivosti servera i aplikativnih platformi, gde se iste mogu na lak način zloupotrebiti koristeći zlonamerne alate. Drugu grupu najčešćih zloupotreba predstavljaju slučajne greške u aplikacijama i greške vezane za dizajn uz nedovoljnu svest o bezbednosti. Kompromitacijom aplikacija i servera na kojima se izvršavaju moguća je dalja infiltracija u druge delove informacionog sistema.

Zašto odgovor na incidente ?

I pored najboljih mehanizama prevencije, incident može da se dogodi. Blagovremeni odgovor na incidente i blagovremeno otklanjanje posledica incidenta je druga ključna komponenta (pored detekcije i prevencije) efikasne zaštite. Opšte je prihvaćena krilatica da nije pitanje da li će se incident dogoditi, već kada. Upravo zbog toga da bi se izbegle negativne posledice po informacioni sistem, moraju se uvesti mehanizmi efikasnog odgovora na incidente.

Šta je sve potrebno za efikasan odgovor na incidente ?

Efikasan odgovor na incidente predstavlja „sveto trojstvo“ tehnologije, ljudstva i procedura:

1. Tehnologija je prva adresa rešavanja problema u IT svetu. Odgovarajuća tehnologija je neophodna za efikasan odgovor na incident, koja će omogućiti određenu automatizaciju, jednostavno blokiranje daljeg širenja incidenta, kvalitetne mehanizme analize itd.
2. Ljudski resursi - Tehnologija neće pružiti nikakvu pomoć ukoliko ne postoje ljudski resursi koji poseduju znanje i koji mogu i znaju efikasno raditi sa tehnologijom. U praksi su se često dešavali ozbiljni incidenti kada je tehnologija na vreme otkrila incident ali niko nije odreagovao. Razlozi mogu biti različiti – od nepostojanja kadrova da se bavi problemima, nepostojanja znanja, nepostojanja fokusa na incident među hiljadama potencijalnih incidenata i drugih zaduženja itd. Incidenti se događaju 24 časa dnevno 7 dana u nedelji i nemaju radno vreme. Efikasan odgovor na incidente zahteva ljudske resurse koji su dostupni 24/7 i koji imaju odgovarajuću ekspertizu u ovoj oblasti. Ovo je često zanemarena komponenta pored tehnologije iako su ljudski resursi često i skuplji i teško je i pronaći odgovarajuće kadrove.
3. Procedure – Da bi se efikasno odgovorilo na incident potrebno je preduzeti brze i odgovarajuće mere. Bez odgovarajućih procedura ni tehnologije ni ljudski resursi neće doneti odgovarajuće rezultate. U sinergiji tehnologije i ljudskih resursa, ključna je i automatizacija koja omogućava da se jednostavni koraci sami preduzmu bez da su izložene potencijalnim ljudskim greškama, a ljudskim resursima „uštedeti“ vreme da mogu da se fokusiraju na zadatke koji zahtevaju humanu ekspertizu.

Kako usluga zaštite aplikacija odgovora na ova pitanja

Zašto je bitna zaštita aplikacija ?

Usluga se fokusira na sveobuhvatnu zaštitu aplikacija.

Da bi se efikasno štitile aplikacije potrebni su različiti mehanizmi i tehnologije koje je potrebno integrisati u celoviti sistem. Primarni cilj usluge je da kroz jedinstveni sistem odgovori na sve sigurnosne izazove koji su vezani za aplikacije.

Koji su specifični rizici vezani za aplikacije ?

Usluga zaštite aplikacija štiti od obe vrste tipičnih rizika – DDoS napada i kompromitacije sistema. U okviru usluge koriste se vodeća tehnološka rešenja iz ove oblasti – tehnologija za zaštitu od DDoS napada i Web Application Firewall (WAF) za zaštitu od kompromitacije koji su integrisani u jednu celinu.

Šta je DDoS napad i koliki rizik predstavlja ?

Zaštita od DDoS napada je složena pošto je teško razlikovati legitimni od zlonamernog sadržaja, pošto u napadu mogu da učestvuju različiti uređaji sa različitih strana sveta. Takođe, kao i kod virusa/malvera pojavljuju se novi tipovi napada (*zero day*) koji ranije nisu bili viđeni, pa ih nije moguće prepoznati na tradicionalan način.

Usluga zaštite aplikacija efikasno štiti od DDoS napada – kako od volumetrijskih tako i do mrežnih (L3/4) i aplikativnih (L7). Zaštita od DDoS napada koristi tehnologiju prepoznavanja napada na bazi ponašanja analizom saobraćaja koji se pokazao najefikasnijim kako i za postojeće „viđene“ načine napada, tako i za nove oblike napada.

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

Koji su rizici vezani za kompromitaciju sistema kroz (web) aplikacije ?

Zaštita od kompromitacije aplikacija se vrši kroz Web Application Firewall (WAF) čiji je cilj smanjenje rizika od specifičnih ranjivosti i njihovih zloupotreba. Najčešće i najbitnije pretnje se klasifikovane u OWASP TOP-10 dokumentu koji se revidira svake godine. Zadatak WAF-a je da eliminiše ove pretnje uz minimizaciju negativnog uticaja na legitiman saobraćaj.

Usluga zaštite aplikacija efikasno štiti od svih pretnji klasifikovanih po OWASP TOP-10 sistemu, a pored toga kroz različite mehanizme kao što su napredno mašinsko učenje kroz analizu saobraćaja, vrši precizno prepoznavanje legitimnog saobraćaja i blokiranje malicioznih aktivnosti. Kroz uslugu se vrši kontinualna adaptacija polisa kako bi se odgovorilo na sve trenutne i buduće pretnje.

Zašto odgovor na incidente ?

Usluga pored detekcije i prevencije obezbeđuje i sve mehanizme za odgovor na incidente. Odgovor na incidente, može da predstavlja skupu investiciju ukoliko organizacije žele same da implementiraju sve mehanizme – 24/7 operativni tim, security stručnjaci, odgovarajuće znanje da se vode timovi i da se

izgrade procedure, neophodna tehnologija i stalno prilagođavanje promenama i novim izazovima. Odgovor na incidente kroz uslugu zaštite radnih stanica eliminiše potrebu za investicijom u ove resurse.

Šta je sve potrebno za efikasan odgovor na incidente ?

Usluga obezbeđuje sve mehanizme koji su neophodni za efikasan odgovor na incident: tehnologiju koja omogućava detekciju samog incidenta, mehanizme daljeg automatskog prikupljanja informacija o incidentu, alate za forenzičku analizu, operativni tim dostupan 24/7 vođen jasnim procedurama, ekspertski tim koji može da odgovori svim izazovima i mehanizme za efikasnu udaljenu blokadu daljeg širenja incidenta.

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.