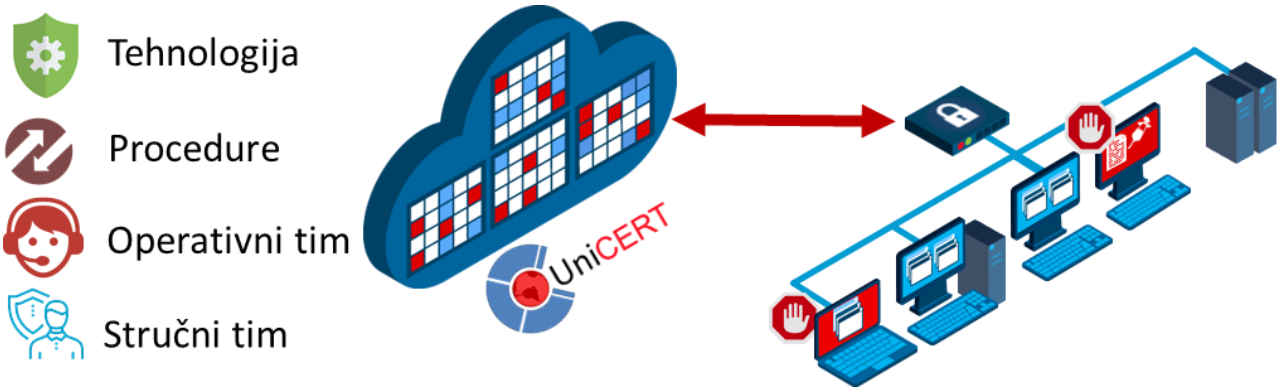
Zaštita radnih stanica

Upravljana usluga prevencije, detekcije i odgovora na incident na radnim stanicama

Opis usluge

Usluga zaštite radnih stanica i servera omogućava najefikasniji vid zaštite informacionog sistema kroz zaštitu samih radnih stanica prevencijom, detekcijom i brzim otklanjanjem posledica u slučaju incidenta. Usluga zaštite radnih stanica 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 instalacijom lakog klijentskog softvera na radne stanice. Sistem vrši prevenciju od svih oblika napada od jednostavnijih do složenih (npr. zaštita od ransomware napada, zaštita od zlonamernog softvera koji vrši praćenje rada na radnoj stanici – prikupljanje lozinki dokumenata itd.), detektuje mogući incident i alarmira operativni tim. Ekspertski tim u slučaju kritičnog incidenta momentalno reaguje, i u konsultaciji sa korisnikom i daje dalje preporuke. U slučaju detektovanog incidenta moguće je momentalno blokiranje radne stanice kako se incident ne bi dalje širio i vrši udaljena forenzička analiza koja je ključna za donošenje odluka o preduzimanju daljih koraka. Veoma veliku vrednost predstavlja i mogućnost korelacije informacija sa drugim uslugama – Email bezbednost i Mrežna bezbednost čime se rizik od pretnji i napada ove vrste skoro potpuno eliminiše. Naravno 100% bezbednost ne postoji, i napad uvek može da se dogodi, ali se kombinacijom ovih usluga praktično eliminišu rizici na svim vektorima – mreži/web-u, email-u i radnim stanicama.



Klijent ima uvid u sve informacije vezane za uslugu kroz korisnički portal. Svi događaji vezani za prevenciju, detekciju i preduzete akcije na radnim stanicama 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 zaštita radnih stanica ?

Radne stanice (desktopovi, laptovi…) a i serveri predstavljaju najčešće ulazne tačke za različite pretnje. Kroz radne stanice se vrši se ljudska interakcija sa informativnim sistemom, što uvek predstavlja i najlakšu i najčešću tačku moguće zloupotrebe. Phisihing mailovi, rizični internet sajtovi, zaražene aplikacije predstavljaju ulazna vrata u radne stanice a kroz iste radne stanice, dalje u ostatak informacionog sistema. Zbog svega toga, u svetlu današnjih pretnji radne stanice upravo predstavljaju delove informacionog sistema koje zahtevaju najefikasniju zaštitu.

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

A antivirus ?

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. Statistika takođe pokazuje da je većina računara koji su se zarazili ransomverom imala instaliran antivirus program.

Kako onda detektovati ?

Deo efikasne zaštite radnih stanica predstavlja prepoznavanje zlonamernih programa po ponašanju. Takvi mehanizmi omogućavaju prepoznavanje ranije nepoznatih oblika napada kao i „mutacije“ virusa (isti virus, sa istim ponašanjem ali sa drugačijim sadržajem koji može u svakoj instanci da bude drugačiji). Takođe, veliku pomoć u detekciji pružaju dinamičke informacije o karakteristikama tekućih napada (indikatori kompromitacije IoC) u regiji i širom sveta na osnovu čega se mogu prepoznati aktuelni napadi.

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 radnih stanica odgovora na ova pitanja

Zašto zaštita radnih stanica?

Usluga se fokusira na zaštitu radnih stanica kao jedno od najefikasnijih pritupa zaštite. Postoje i drugi bezbednosni izazovi koji se moraju rešavati drugim pristupom (zaštita od curenja informacija, zaštita infrastrukture od mrežnog ili aplikativnog napada itd.) ali u skladu sa današnjim trendovima bezbednosnih izazova upravo najviše nedostaje ovaj vid zaštite i upravo ovaj vid zaštite može da eliminiše veliki procenat bezbednosnih rizika.

A antivirus ?

Antivirus je sam po sebi neefikasan u eliminaciji bezbednosnih rizika, ali je i dalje delimično potreban. Usluga pored naprednih oblika prevencije i detekcije uključuje u sebi i klasičan antivirus, što eliminiše potrebu za troškovima za druga antivirus rešenja.

Kako onda detektovati ?

Kako efikasna detekcija zahteva spoj različitih metoda, usluga zaštite radnih stanica upravo kombinuje različite mehanizme koji zajedno doprinose visokoj sigurnosti sistema. Od klasičnih metoda detekcije na bazi signatura, detekcije prisustva indikatora kompromitacije na bazi relevantnih, dinamičkih „obaveštajnih“ podata iz regiona i iz sveta, na bazi prepoznavanja oblika ponašanja malicioznog koda uz blokiranje njihovog dejstva. 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 korisnika, analizira događaje i reaguje po potrebi.

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.