Konferencija FSec - Intervju sa Tonimirom Kišasondijem

U sklopu najave konferencije o informacijskoj sigurnosti FSec2017 razgovarali smo s doc. dr. sc. Tonimirom Kišasondijem s Fakulteta organizacije i informatike iz Varaždina, predsjednikom organizacijskog odbora i jednim od utemeljitelja konferencije, koji nam je odgovorio na par pitanja vezanih uz samu konferenciju.

Poštovani gospodine Kišasondi, zahvaljujemo na trudu i vremenu koje ste izdvojili u vrijeme zadnjih priprema za konferenciju. FSec2017 je najvažnija nezavisna konferencija o informacijskom sigurnosti u Hrvatskoj. Možete li na opisati kako su izgledali počeci 2010. godine i kako je došlo do ideje da se organizira ovakva konferencija?

Ideja za FSec je nastala nakon posjeta mene i mojeg prijatelja Kosta na 27th Chaos Communication Congress u Berlinu, konferenciju koja uz informacijsku sigurnost ima dosta drugih interesnih područja, većinom vezanih uz "hakerski" mentalitet. To je ostavilo dosta veliki dojam na mene. Okupljanje preko 10 000 ljudi na jednom mjestu, koje zanima struka, prijenos znanja i kako da nešto nauče. Zezancija je pala na temu zašto to nemamo kod sebe u Hrvatskoj i 9 mjeseci nakon toga, organizirali smo FSec paralelno s FOI-evom znanstvenom konferencijom CECIIS prije 7 godina. Bilo nas je oko 40-ak. Stali smo u kafić na Fakultetu.

Od 40 smo linearno rasli prema 150 i u jednom trenu jednostavno nismo mogli više ostati na FOI-u jer je najveća dvorana na Fakultetu postala premala te smo konferenciju morali preseliti u veći prostor. Odluka je pala na HNK Varaždin u kojem smo drugu godinu za redom. I eto nas tu, nije par desetaka tisuća ljudi kao na DEFCON-u ili CCC-u ali prešli smo 300 ljudi koje zanimaju teme iz informacijske sigurnosti u RH. Ako uzmemo u obzir da konferencija nema komercijalni interes nego skupljamo sponzorstva i ulažemo sve u unaprjeđenje konferencije, mi smo zadovoljni.

Kakvi su Vaši dojmovi nakon šest održanih FSec konferencija? Gdje vidite FSec za pet godina?

Nakon 6 konferencija dojmovi su kako je to puno posla. Iz jednog "underground" okupljanja smo se dotakli i korporativnih tema i stvari koje zanimaju korporativnu publiku do tema koje su bitne za cjelokupnu nacionalnu sigurnost iz aspekta informacijske sigurnosti. Trenutno imamo u programu svega, od jako tehničkih tema do organizacijskih tema, za svakoga ponešto. Plan za 5 godina je raditi isključivo na kvaliteti sadržaja koja se plasira posjetiteljima. To znači i promjene, ali ipak treba eksperimentirati.

Ono što FSec predstavlja je jednu platformu gdje se okuplja ekipa koja dijeli interes dijeljenja znanja i ekspertizu u području informacijske sigurnosti. Od početne trojke, Vlatka Košturjaka, Igora Vuka i mene, koja je osnovala prvi FSec, polako smo proširivali organizacijski odbor. Tu je i veza NCERT-a i FSec-a. Predavanje o stanju informacijske sigurnosti u RH je na prvoj konferenciji držao vaš kolega iz NCERT-a Domagoj Klasić, a do sve većeg uključivanja NCERT-a u FSec dolazi uključivanjem vaših kolega Tonija Gržinića i Marka Staneca u organizacijski tim konferencije.

U organizaciju su se uključivali kroz godine i drugi, Tomislav Androš, Ksenija Cajzek, Dalibor Dukić,

Mario Harjač, Vitomir Margetić, Dobrica Pavlinušić, Slaven Smojver, Ivan Špoljarić, Miroslav Štampar, Ivo Ugrina, Neven Vučinić, Vedran Vukovac i Bojan Ždrnja. Ima nas 18, ali posla je za barem 40 ljudi. Ja sam izuzetno zahvalan cijelom organizacijskom odboru konferencije jer to bez njih to ne bih mogao napraviti.

Ovogodišnja konferencija ugošćuje značajne predavače na velikom broju predavanja i radionica. Kakva su Vaša očekivanja od ovogodišnje konferencije? Želite li neke teme posebno izdvojiti?

Mislimo da svatko može pronaći svoju nišu i interes te da imamo dosta dobro pokrivene teme. Od organizacijskih predavanja poput "How we do CISO @ KPN" gđe Jaye Baloo, "Trouble with updates" Ryana Lackeya, "Targeted Attacks in 2017" Aimea iz Kasperskog do tehničkih predavanja o fuzzanju browsera Ivana Fratrića iz Google Project Zeroa, "HTTP for good and bad" Xaviera Mertensa, napadima na DVR sustave Istvana Totha. Dotaknuli smo se dvije velike teme, GDPR-a kroz okrugli stol i radionicu o GDPR-u te okrugli stol o direktivi PSD2 koja se odnosi na servise plaćanja. Čak imamo i predavanje o NIS direktivi EU. Gotovo cijeli spektar interesa iz informacijske sigurnosti je pokriven i skoro svatko može pronaći predavanje koje mu je interesantno. Imamo 2 dana i 3-4 tracka predavanja, tako da je sadržaja više nego dovoljno. Dobra stvar je da snimamo neka predavanja pa ljudi mogu popratiti ono što ih zanima ako propuste neko predavanje.

Smatrate li kako se sigurnosti informacijskih sustava pridaje dovoljno pažnje u svakodnevici? Na koji način možemo, na razini cjelokupne populacije, podići razinu sigurnosti računalnih sustava?

Odgovor na ovo pitanje je: kako tko. Ne želim posebno neke hvaliti niti prozivati. U svojem poslu gdje u sklopu laboratorija za otvorene sustave i sigurnost radimo sigurnosne provjere, u praksi sam vidio vrlo dobro zaštićenih sustava gdje to nisam očekivao do užasno ranjivih sustava gdje sam očekivao daleko veću razinu sigurnosti i svijesti. Mislim da je vrijeme da u informacijskoj sigurnosti počnemo pričati o odgovornosti. Auto industrija je došla do toga, prije ili kasnije će i IT industrija morati prići tome.

Jedno od tih pitanja je bi li poduzeća koja razvijaju aplikacije za svoje klijente trebala razvijati sigurne aplikacije? Smatra li se sigurnost sustava jednako funkcionalnim zahtjevom kao i ispravan rad aplikacije? Imamo sve više priče o novim tehnologijama kao što su autonomna vozila, bitcoin i blockchain. U tim domenama softverska ranjivost može biti iskorištena za ubojstvo ili za krađu više milijuna eura. Prvo još nismo vidjeli kako bi znali za sigurno, ali drugo smo vidjeli kroz DAO hack i ranjivost u multi-sig verifikaciji ethereum walleta. Zadnjim napadom su kriminalci oštetili 3 walleta za oko 32 milijuna USD, a to je tek izolirani incident i početak. Interesantno je pitanje što će se dogoditi kada te tehnologije dođu u široki opticaj na međunarodnoj razini. SWIFT je prikazao dokaz koncepta na Burrow blockchainu, ISO ima radnu skupinu o blockchain / ledger specifikaciji i prije ili kasnije će i klasične mreže poput SWIFT-a prijeći na blockchain.

Cijeli će ekosustav postati interesantniji zbog GDPR-a prema kojem su predviđene drakonske kazne u slučaju gubitka osobnih podataka klijenta. Uzmite kao primjer situaciju kao u SAD - curenje podataka demokratskog komiteta i podataka o sigurnosnim provjerama zaposlenih u državnoj upravi. To otvara i nove mogućnosti u haktivizmu i korporativnoj špijunaži kroz namjerna curenja osobnih podataka s ciljem financijske štete ili novih oblika ucjene. Umjesto kriptiranja podataka, napadaču je dovoljno da prijeti javnom objavom osobnih podataka klijenta. Definitivno živimo u interesantnim vremenima punima novih izazova.

Podizanje razine sigurnosti je jednostavno, treba pridodati važnost informacijskoj sigurnosti, podizati svijest kod zaposlenika i managementa, a tu je bitan pristup prema kojem zaposlenike ne treba tretirati nekompetentne dronove, nego ih motivirati da budu bolji i da budu proaktivni u području informacijske sigurnosti. Prije 3 FSeca je CISO jedne veće banke u Sjedinjenim Američkim Državama govorio o tome kako imaju program "guardiana" prema kojem zaposlenici koji utvrde mailove s

phishing porukama ili malicioznim kodom dobivaju bonuse kada incidente prijave uredu informacijske sigurnosti koji ih blokira diljem tvrtke. Tehničke mjere u informacijskoj sigurnosti su bitne, ali ključ su još uvijek ljudi, procesi i sistematičnost u primjeni slojevite zaštite.

pon, 2017-09-04 15:35 - Uredništvo**Vijesti:** Sigurnost [1]
Događanja [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: FSec [3]
Tonimir Kišasondi [4]
intervju [5]

Source URL: https://sysportal.carnet.hr/node/1757

Links
[1] https://sysportal.carnet.hr/taxonomy/term/13
[2] https://sysportal.carnet.hr/taxonomy/term/43
[3] https://sysportal.carnet.hr/taxonomy/term/127
[4] https://sysportal.carnet.hr/taxonomy/term/130
[5] https://sysportal.carnet.hr/taxonomy/term/131