Što smo naučili iz napada na SCADA/DCS sustave?

What are the lessons learned from the attack on SCADA/DCS systems?

Krešimir Pešice
S.C.A.N. d.o.o. Hrvatska
kresmir.pesice@scan.hr

Ključne riječi: kibernetička sigurnost, SCADA/DCS sustavi, energetski sektor

Key words: cyber security, SCADA/DCS systems, energy sector

Sažetak

Industrijski sustavi automatizacije upravljanja nezaobilazan su dio svakog postrojenja u energetici. U praksi se pokazalo da kibernetički napadi na takva postrojenja mogu rezultirati vrlo ozbiljnim posljedicama uključujući fizičku destrukciju opreme ili cijelog postrojenja. Iako kibernetički napadi na informatičke sustave imaju nesagledive posljedice na poslovanje tvrtki, u ovom članku usmjeriti ćemo se na ICS (Industrial Control System) sustave koji upravljaju opremom i postrojenjima.

Sve tvrtke u energetskom sektoru su obveznici primijene Zakona o kibernetičkoj sigurnosti, a ona se ne smije shvaćati površno, poglavito potencijalni kibernetički napadi na SCADA sustave koji za posljedicu mogu imati uništenje cijelih postrojenja. U opasnosti su ljudski životi, mogući su veliki ekološki incidenti i dakako, goleme materijalna šteta koje se mjere u desecima miliona eura.

Abstract

Industrial automation system is an indispensable part of any energy facility. In practice cyber-attacks on such facilities can result in very serious consequences including physical destruction of equipment or the entire facility. Although cyber-attacks may have unforeseen consequences on business operations, this paper will focus on Industrial Control Systems for equipment and facilities.

All energy companies are obliged to comply with the Cyber Security Act, and it should not be implemented superficially, particularly considering potential cyber-attacks on SCADA systems which can cause the destruction of entire facilities. This can result in threats to human lives, large-scale environmental incidents and huge material damages measured in tens of millions of euros.

1. Uvod

Kibernetička sigurnost je često korišten pojam u različitim kontekstima. Kada se kaže kibernetička sigurnost svatko ima različito razumijevanje tog pojma. Kibernetičkom sigurnošću definirati ćemo mjere zaštite računalnih sustava od neovlaštenog pristupa

podatcima ili napada na sustav. Na početku ovog preglednog članka citirat ćemo izjavu američkog profesora informatike na Sveučilištu Purdue i vodećeg stručnjaka za računalnu sigurnost Eugene Howard Spafforda „Jedini informacijski sustav koji je zaista siguran je onaj koji je isključen iz napajanja, zaliven u betonski blok te zaključan u sobu obloženu olovom koju čuvaju dobro naoružani čuvari – čak ni tada, ne bih se baš kladio na njega".

Industrijski sustavi automatizacije upravljanja (u daljnjem tekstu: ICS) nezaobilazan su dio svakog postojanja u energetici. Pokazalo se u praksi da kibernetički napadi na takva postrojenja mogu imati vrlo ozbiljne posljedice, uključujući fizičku destrukciju opreme ili cijelog postrojenja. Iako kibernetički napadi na informatičke sustave (u daljnjem tekstu: IT) imaju velike posljedice na poslovanje tvrtki, u ovom članku u središtu pozornosti biti će ICS sustavi koji upravljaju opremom i postrojenjima.

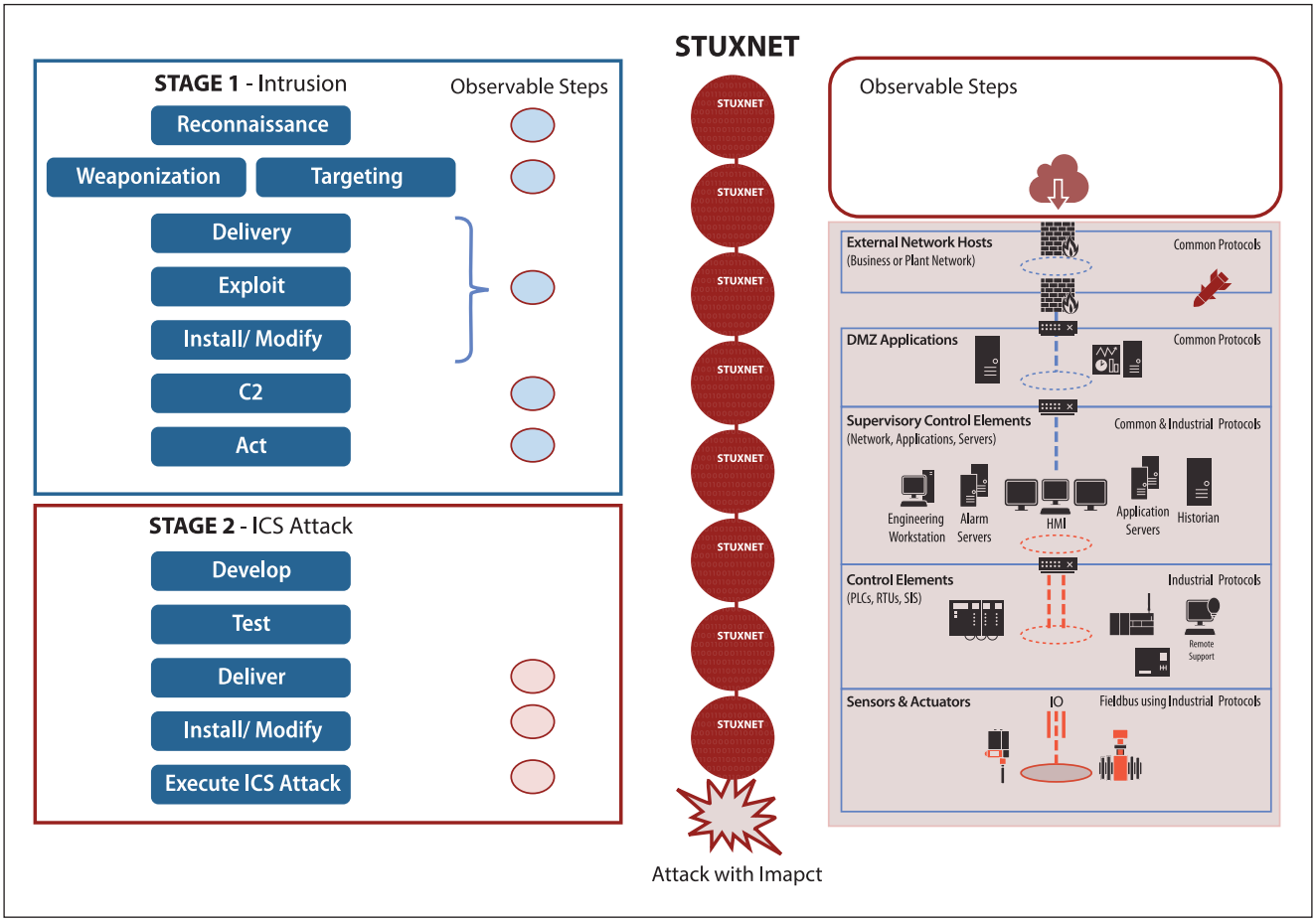
Čak 87 posto višeg menadžmenta u industriji nafte i plina izjasnilo se, da je njihova tvrtka imala kibernetičke incidente u posljednjih 12 mjeseci. (Kroll Global Fraud & Risk Report, 2018.).

2. Tehnike kibernetičkih napada na ICS sustave

Prvi zabilježen slučaj kibernetičkog napada s posljedicama fizičke destrukcije dogodio se u Iranu na postrojenju za obogaćivanje urana. S obzirom na različite proturječne i nepouzdane informacije referirati ćemo se na članak „The History of Stuxnet: Key Takeaways for Cyber Decision Makers" pripremljen za „Cyber Conflict Studies Association".

Nakon početne faze ulaska u sustav putem Windows računala, računalni crv (vrsta zloćudnog računalnog koda) je uspio doći do ICS sustava (Siemens PCS7). Uz mnoge druge napredne funkcionalnosti, sa stanovišta kibernetičke sigurnosti ICS sustava je najzanimljivija sposobnost za napade dugog stupnja. (Slika 1. Stuxnet ICS Kill Chain).

Stuxnet je prvi poznati zloćudni softver namjenski dizajniran za ICS sustave. U drugom stupnju napada izmijenio je programe na DCS kontrolerima na način da izazove fizičko uništenje opreme. Uz mnoge kontraverze o porijeklu i sposobnostima napadača. Stuxnet je dokazao da je moguće izvesti napad koji će imati za posljе-



Slika 1. ICS Kill Chain

dicu fizičko uništenje postrojenja sa svim posljedicama po život i zdravlje ljudi. Ovaj napad je jasno upozorenje ICS zajednici da pitanje kibernetičke sigurnosti treba podignuti na potpuno novu razinu prioriteta.

Napraviti softver koji može fizički uništiti postojanje je potpuno nova razina opasnosti do tada poznata samo u teoriji. Napadač ne samo da je odlično poznavao Siemensov sustav, već je odlično poznavao tehnološki proces i fizički dizajn samog postojanja koje je bilo cilj napada. Osim tima stručnjaka koji poznaju tehnološki proces, vrlo vjerojatno je u svojem testnom postrojenju napadač napravio identičnu centrifugu za obogaćivanje urana. Za napad se pripremio serijom testova kako bi se uvjerio da će određena promjena programa na kontroleru izazvati fizičko uništenje opreme. Sva moderna postrojenja imaju brojne mehanizme pasivne i aktivne sigurnosti. Nije ih lako zaobići i dovesti postrojenje u nesigurnost na način da se zaobiđu svi mehanizmi sigurnosti i izbjegne sigurnosno zaustavljanje. Potrebno je odlično poznavanje postrojenja kako bi se iskoristila slabost u njegovom dizajnu, a koja bi se mogla iskoristi za uzrokovanje fizičke štete.

Iako je Stuxnet izazvao veliku pozornost informatičke zajednice, smatramo da je sposobnost napada na ICS sustav puno značajniji. Postavljaju se brojna pitanja. Kako je računalni crv došao na postrojenje koje nije spojeno na internet niti nikakvu poslovnu mrežu? Kako je znao doći do ciljanog dijela računalne mreže i određenih kontrolera? Kako je znao kako je napravljen program za upravljanje centrifugama?

Početna pretpostavka o širenju računalnog crva putem USB ključa izaziva sve više sumnji kao netočna. Vjerojatno je inicijalni vektor napada prijenosno računalo inženjera.

Procjenjuje se da je računalni crv Stuxnet pronađen na još najmanje 100.000 lokacija u Iranu, Indiji, Europi i Sjedinjenim Američkim Državama. S obzirom da je bio napravljen za specifične namjere drugdje u svijetu nije izazvao slične posljedice.

Iako specifičan, slučaj Stuxneta i na prvi pogled se čini izuzetkom. Pokazati će se kao „zvono na uzbunu“ i potaknuti će mnoge napore kako bi se civilna postrojenja učinila otpornijim na kibernetičke napade. Države su ubrzale uvođenje regulativa vezanih uz kibernetičku sigurnost ICS sustava. Proizvođači ICS sustava i opreme ozbiljnije su počeli shvaćati kibernetičke prijetnje.

U kibernetičkoj sigurnosti podatci o žrtvi napada nisu bitni. Iako širu javnost najviše zanima ime žrtve, u praksi vrlo rijetko govorimo o imenima napadnutih tvrtki. Žrtva je uvijek žrtva, bez obzira koliko je bila loše pripremljena za odgovor na incident, nije zaslužila

dodatno sramoćenje u medijima. Time smo izgradili sustav međusobnog povjerenja. Žrtve ne prikrivaju napade da bi zaštitile vlastitu ugled, a istodobno, podiže se razina povjerenja unutar sektora ICS kibernetičke sigurnosti. Potrebna je duga i temeljita istraga da bi se pouzdano utvrdio uzrok incidenta. Zbog nedostatka stručnog kadra i mogućnosti kvalitetne istrage uzroka incidenta nerijetko vlasnici postrojenja krivo zaključe da je razlog incidenta greška u održavanju ili slično. Primjer napada na čeličanu u njemačkoj i destrukcija visoke peći.

Važno je poznavati taktike, tehnike i procedure napada (TTP), jer pomoću njih provjeravamo kakve bi učinke imao takav napad na naše postrojenje i koje su naše sposobnosti da se uspješno obranimo.

U slučaju Stuxnet Siemens se našao na udaru s obzirom da se radilo o njihovom sustavu i opremi. To je potpuno neopravdano. Pomnijom analizom može se zaključiti da se to moglo dogoditi na bilo kojem sustavu drugih proizvođača.

Nije dugo trebalo čekati da se drugi proizvođači ICS sustava nađu na udaru. Za razliku od Stuxneta koji je bio vrlo sofisticiran, Havex – drugi poznati zlćudni računalni kod sa specifičnom namjerom ugrožavanja ICS sustava je iznimno jednostavan. Otkriven je 2014., a koristi se od 2013. godine. Napravljen je s namjerom prikupljanja informacija o ICS sustavima žrtava, uz pretpostavku da bi se te informacije mogle koristiti za napade. Korištene su dobro poznate ranjivosti. Pojednostavljeno rečeno zlćudni kod ugrađen je u originalni softver nekoliko velikih proizvođača ICS sustava. Žrtve su instalirale softver skinut sa stranica proizvođača ICS sustava, ne sumnjajući da je softver kompromitiran. Iskorišten je jedan od stupova povjerenja u proizvođače ICS sustava. Zlćudni kod se našao u lancu opskrbe. Oprema dobavljena od velikih isporučitelja ICS sustava nikad nije dovođena u pitanje kao vektor napada. U ovom slučaju napadač nije koristio složen zlćudni kod kao u slučaju Stuxnet. Jeftinije i

jednostavnije je bilo koristiti povjerenje koje imamo u dobavljače i proizvođače.

Kao ilustraciju navest ćemo treći primjer ICS zloćudnog koda poznatog kao Trisis. Napravljen sa specifičnom svrhom napada na SIS sustave (Safety Instrumented System). Imao je značajan učinak u jednoj naftnoj kompaniji iz Saudijske Arabije. Uloga SIS sustava je da u slučaju opasnosti po postrojenje, zaustavi postrojenje na siguran način. Kompromitacija SIS sustava utječe na vjerojatnost i posljedice industrijske nesreće. Standard funkcijske sigurnosti „IEC 61511 Functional Safety – Safety Instrumented Systems for the Process Industry Sector" navodi procjenu rizika kibernetičke sigurnosti kao obvezu. Tehnička preporuka ISA-TR84.00.09-2017. „Cybersecurity Related to the Functional Safety Lifecycle" pruža smjernice kako implementirati, upravljati i održavati sigurnosne kontrole („Safety Control") na siguran način. Kibernetička sigurnost ICS sustava je čvrsto vezana na funkciju sigurnost.

Svrha članka nije pobrojati sve vrste zloćudnog koda, već zorno ilustrirati stanje kibernetičke sigurnosti ICS sustava u svijetu. Današnji napadači na postrojenja u industriji nafte i plina, ne samo da poznaju ICS sustave različitih proizvođača, već u svom timu imaju inženjere koji poznaju procese i tehnologiju postrojenja. Trenutno u svijetu postoji nekoliko skupina koje su demonstrirale sposobnosti napada na ICS sustave u industriji nafte i plina. Djeluju na različitim zemljopisnim područjima i pod određenim geopolitičkim okolnostima. Od toga minimalno tri skupine su aktivne na prostoru Europe

Osim specifičnih ICS zloćudnih računalnih programa, ICS sustavi su također osjetljivi na zloćudni računalni kod namijenjen poslovnim informatičkim sustavima. Ovdje se ponajprije misli na „Cryptolocker Ransomware". Zloćudni kod koji kriptira podatke na računalu i blokira korištenje računala, samim time i ICS programa na njemu.

Sve nabrojene ugroze pokazale su nužnost sistematskog i sveobuhvatnog pristupa kibernetičkoj sigurnosti ICS sustava.

3. Kako se nositi s izazovom kibernetičke sigurnosti ICS sustava?

Problem kibernetičke sigurnosti ICS sustava shvaćen je vrlo ozbiljno u široj zajednici. Vrlo rano se shvatilo da norme kibernetičke sigurnosti iz informatičkih sustava nisu dovoljne za ICS sustave. Informacijska sigurnost dugo postoji kao važan faktor u IT okruženju. Norma ISO 27001 upravljanje informacijskom sigurnošću je vrlo široko prihvaćen dokument. Iz tog razloga su i razumljive inicijative IT sektora prema ICS sustavima i pokušaji da se preslikaju obrasci i mjere IT-a u ICS okruženje. U svakom slučaju valja uključiti kolege iz IT-a u programe kibernetičke sigurnosti ICS sustava. Oni mogu biti važan član tima za ICS kibernetičku sigurnost.

4. Zakonska regulativa

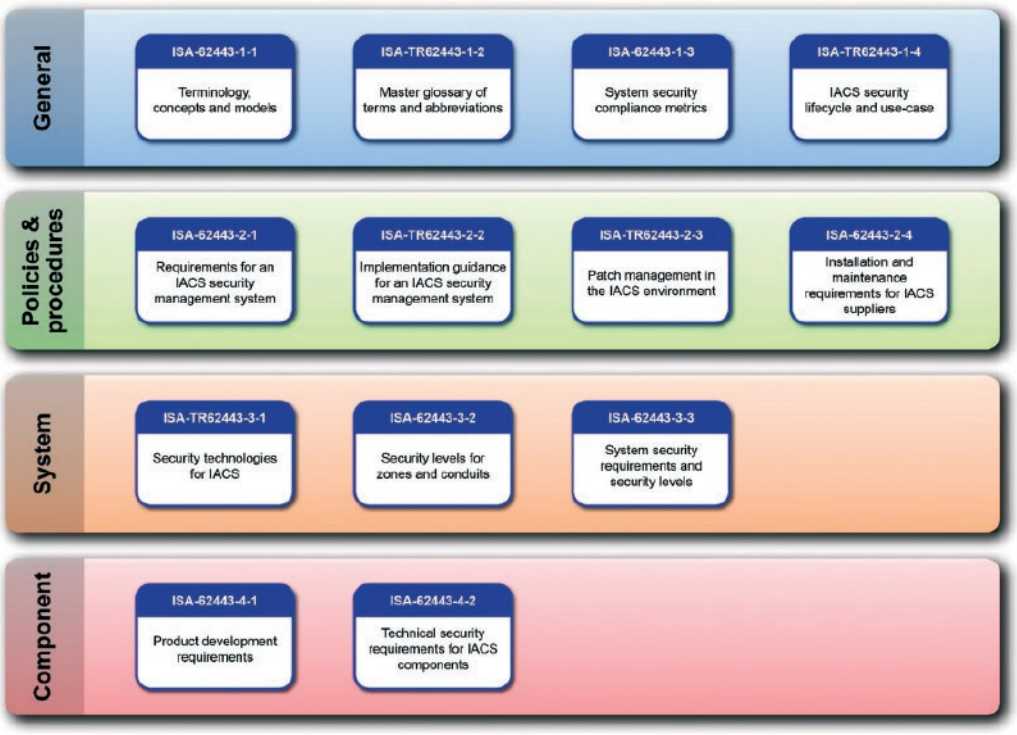
Europska unija je 2016. godine donijela NIS direktivu („Directive on Security of Network and Information Systems"). Hrvatska je kao članica EU implementirala NIS direktivu putem „Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga" i „Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga." Između ostalog, cijeli je energetski sektor obveznik tog zakona. Postojeći zakon je tek prvi korak. Europska unija radi na mnogim novim regulativama.

Mnoge članice EU krenule su u implementaciju NIS direktive u energetski sektor putem norme IEC 62443. EU radi na standardizaciji gdje se također norma IEC 62443 želi uvesti kao standard kibernetičke sigurnosti ICS ustava. (https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/)

Zapravo ne postoji niti jedna druga norma koja se odnosi na kibernetičku sigurnost ICS sustava, tako da je odabir norme IEC 62443 zapravo logičan sam po sebi. Velika Britanija je prihvatila američki NIST SP 800-82, „Guide to Industrial Control Systems (ICS) Security" (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf). NIST standard se vrlo sličan IEC 62443 standardu, ali je prilagođen specifičnom kontekstu SAD-a.

U Hrvatskoj trenutno najozbiljnije napore u uvođenju norme IEC 62443 ulaže Hrvatska Elektroprivreda. Elektrane su vrlo složeni sustavi i potencijalne mete visoke vrijednosti za napadače.

Sistem integratori kao tvrtke koje instaliraju i održavaju ICS sustave intenzivno razvijaju svoje sposobnosti u području kibernetičke sigurnosti. Čest je slučaj da tvrtka sistem integrator isporučitelj zna više o ICS sustavu od samog krajnjeg korisnika. Pojedini hrvatski ICS sistem integratori aktivno prate trendove u kibernetičkoj sigurnosti. Osim što su duboko povezani s proizvođačima sustava, odlično poznaju i tehnološke procese s kojima njihovi sustavi upravljaju. Ulaganje u stručnjake za kibernetičku sigurnost ICS sustava je konstantan napor i značajan trošak.



Slika 2.
Struktura norme
IEC 62443

Norma IEC 62443 Security for Industrial Automation and Control Systems najšire je prihvaćen standard kibernetičke sigurnosti. Obuhvaća krajnje korisnike ICS sustava, sistem integratore, proizvođače i same proizvode.

Trenutačno nema značajnog proizvođača ICS sustava koji se ne ulaže znatne napore u kibernetičku sigurnost i IEC 62443 normu.

U razvoju same norme IEC 62443 aktivno sudjeluju i stručnjaci iz najvećih kompanije u sektoru nafte i plina. Široko je prihvaćen u nizu industrija, ali primarno je vezana uz procesnu industriju.

5. Kako se obraniti ako ne znamo što branimo?

Prvi korak upravljanju kibernetičkom sigurnošću je znati što branimo. Koje su granice sustava? Od čega sustav sastoji?

Za razliku od IT sustava, gdje postoji cijeli niz automatiziranih alata za prikupljanje podataka o komponentama sustava. U ICS svijetu to nije moguće napraviti automatski. Potrebno je prikupiti potpune informacije o opremi i izvedenom stanju postrojenja. Često se događa da dokumentacija izvedenog stanja ne odgovara trenutnom stanju. Osim cijelog niza izmjena koje su napravljene a nisu dokumentirane, postoje slučajevi potpunog nepoznavanja čemu sve neki dio kontroler služi i gdje se fizički nalazi. Iz tog razloga je proces procjene rizika kibernetičke sigurnosti za industrijska postrojenja vrlo često mukotrpan i dug.

Tim stručnjaka za procjenu kibernetičke sigurnosti ICS sustava minimalno se sastoji od:

Voditelja tima certificiranog za procjenu rizika kibernetičke sigurnosti ICS sustava;

- Automation / Controls Inženjera;
- Inženjera za računalne mreže;
- Eksperta za kibernetičku sigurnost ICS sustava;
- Eksperta za sigurnosti tehnološkog procesa;
- Iskusnog operatera sustava.

Takav tim može sagledati sve aspekte rizika i povezati kibernetičku sigurnost s drugim sustavima kvalitete i tehničkim normama.

6. Četiri razine kibernetičke sigurnosti

Uvođenje mjera kibernetičke sigurnosti u postojeća postrojenja vrlo je složeno i dugotrajno. Osim neažurne dokumentacije, problem je što se pri dizajnu sustava nije vodilo računa o kibernetičkoj sigurnosti. Potrebno je raditi mnoge kompromise i vrlo skupe zahvate koji ne bi bili potrebni da se od početka vodilo računa o kibernetičkoj sigurnosti.

Proizvođači ICS ustava razvili su cijeli niz funkcionalnosti kibernetičke sigurnosti svojih sustava. S obzirom da investitori ne definiraju željenu razinu kibernetičke sigurnosti, niti u investiciji planiraju financijska

sredstva za kibernetičku sigurnost, propuštaju priliku da se u ranoj fazi, kada je najjeftinije i najučinkovitije, implementira željena razina kibernetičke sigurnosti. Norma IEC 62443-3-3 je vrlo precizna u smislu koji su kriteriji za određivanje razine kibernetičke sigurnosti. Postoje četiri razine sigurnosti:

SL1 – Zaštita od nehotičnih i slučajnih pogrešaka (individualne greške operatera);
SL2 – Zaštita od međunarodnih skupina koje vrše jednostavne napade koristeći male resurse, opće vještine i nisku motivaciju za napad (cyberkiminal);
SL3 – Zaštita od međunarodnih skupina koje vrše sofisticirane napade korištenjem značajnih resursa, raspolažu znanjima o ICS sustavima i imaju srednju razinu motivacije (hacktivisti, teroristi);
SL4 – Zaštita od međunarodnih skupina koje vrše sofisticirane napade korištenjem velikih resursa, raspolažu znanjima o SCADA sustavima i imaju visoku razinu motivacije (nacionalne države).

Pri odabiru željene razine kibernetičke sigurnosti nužna je odluka najvišeg managementa.

7. Kibernetičke sigurnosti ICS sustava nema alternativu

S obzirom na sve veće opasnosti i sve strože zakonske regulative uvođenje programa kibernetičke sigurnosti ICS sustava nema alternativu. Treba početi od pitanja: koga zvati u slučaju kibernetičkog napada na ICS sustav? Logičan korak je ponajprije uključiti tvrtku koja je isporučila i održava sustav. ICS sistem integratori su svugdje u svijetu na prvoj liniji. Osim poznavanja ICS sustava i specifičnosti njihove kibernetičke sigurnosti, oni poznaju vaš tehnološki proces i kontekst u kojem se odvija. U skladu sa svjetskim trendovima, hrvatski ICS sistem integratori razvijaju timove za kibernetičku sigurnost kako bi cjelovito mogli zadovoljiti potrebe krajnjih korisnika i proizvođača ICS sustava u njihovoj evoluciji sposobnosti kibernetičke sigurnosti.

Upravljanje incidentima kibernetičke sigurnosti i oporavak od napada tema je aktualnih rasprava. Treba naglasiti da bez odgovarajuće procjene kibernetičke sigurnosti nije moguće napraviti realan i provediv plan djelovanja u slučaju incidenta. Razgovarajte sa svojim sistem integratorima ICS sustava, raspitajte se koje su njihove mogućnosti i krenite planirati, budžetirati.

8. S.C.A.N. je vodeći hrvatski sistemski integrator na području instrumentacije i sustava upravljanja

S.C.A.N. je vodeći hrvatski sistemski integrator na području instrumentacije i sustava upravljanja, specijaliziran za pružanje rješenja automatizacije procesa, uglavnom u sljedećim granama industrije:

- proizvodnja nafte i plina, na kopnu i na moru;
- rafinerije nafte;
- naftni i UNP terminali;
- naftovodi i plinovodi;
- razna petrokemijska i kemijska postrojenja.

Glavne djelatnosti tvrtke S.C.A.N. su:

- projektiranje i konzultantske usluge;
- integracija sustava;
- kibernetička sigurnost;
- održavanje instrumentacije i sustava upravljanja;
- tehnička podrška.

U gotovo 30 godina postojanja S.C.A.N. je implementirao preko 100 ICS sustava različitih generacija, najpoznatijih svjetskih proizvođača:

- Emerson DeltaV;
- ABB Advant, 800xA;
- Yokogawa;
- Različiti PLC sustavi (Mitsbishi, Allen Bradley, Siemens);
- PCVue SCADA system;
- iFIX SCADA system;
- Factory Link SCADA system.

U području kibernetičke sigurnosti ICS sustava SCAN nudi usluge:

- Procjene rizika sukladno normi IEC 62443 i drugim relevantnim propisima;
- Projektiranje sustava kibernetičke sigurnosti;

- Implementaciju i održavanje sustava kibernetičke sigurnosti.
- Verifikaciju implementiranih mjera i provjera učinkovitosti mjera kibernetičke sigurnosti.

9. Projekt „Inovativno rješenje za upravljanje kibernetičkom sigurnosti industrijskih sustava automatizacije postrojenja i procesa“

Tvrtka S.C.A.N., kao najveći hrvatski integrator ICS sustava u industriji nafte i plina je 2019. godine pokrenula snažan investicijski ciklus u područje kibernetičke sigurnosti.

Kao nastavak tih napora tvrtka S.C.A.N. zajedno s fakultetom Elektrotehnike i računarstva Sveučilišta u Zagrebu pokrenula je u kolovozu ove godine istraživačko razvojni projekt u području kibernetičke sigurnosti ICS sustava. Realizacija projekta pod nazivom „Inovativno rješenje za upravljanje kibernetičkom sigurnosti industrijskih sustava automatizacije postrojenja i procesa“ važan je korak u razvoju tvrtke S.C.A.N. Tvrtka planira nastaviti unaprjeđivati rješenje i u budućnosti, ali i razvijati komplementarne proizvode te nove inovacije s obzirom na potrebe tržišta kibernetičke sigurnosti ICS sustava.

Ukupna vrijednost projekta iznosi 22.591.320,10 HRK. Udio sredstava kojima se financira projekt iz Europskog fonda za regionalni razvoj iznosi 14.079.545,67 HRK. Predviđeno trajanje projekta 36 je mjeseci.

Radi se o jednom od najvećih, ulaganja u istraživanje i razvoj rješenja kibernetičke sigurnosti ICS sustava u Republici Hrvatskoj. U SCAN-u su ponosni što je kvaliteta njihovog projekta i ekspertiza članova projektnog tima prepoznata, a to potvrđuje i sufinanciranje projekta od strane Europskog fonda za regionalni razvoj.

U sklopu projekta instalirati će se testno postrojenje sastavljeno od ICS sustava najvećih svjetskih proizvođača. Moći će se testirati sigurnost sustava prema različitim scenarijima iz prakse, uvježbavati timove za detekciju napada, razrađivati scenarije odgovora na incidente te stvoriti centar kompetencija kako bi mogli podržati klijente na njihovom putu prema uvođenju sustava upravljanja kibernetičkom sigurnošću u skladu sa svjetskim standardima.