Securitatea Cibernetică în Mediul Industrial

Palatul Cesianu-Racoviță, 04 Aprilie 2017, București

Comunicat post-eveniment

În 4 aprilie, 2017, la Palatul Cesianu-Racoviță, ISACA România, a inițiat o dezbatere pe problema digitalizarii proceselor industriale și securitatea acestora susținută de Hidroelectrica, Transelectrica, Servicul Român de Informații (SRI), PwC, EY și Enevo Group.

Cu o prezență de peste 60 de participanți, evenimentul a reunit reprezentanți ai managementului din principalele companii de utilități și energie din România precum Hidroelectrica, Arcelor Mittal, Transelectrica sau Conpet, dar și reprezentați a unor instituții importante precum SRI, Ministerul de Interne, Guvernul României sau Ambasada Statelor Unite la București.

Întâlnirea a venit întru-un context în care sistemele industriale fizice și digitale devin din ce în ce mai interconectate, iar complexitatea acestora creste exponențial. Fiecare investiție în tehnologie, pe care o companie industrială sau de utilități o efectuează pentru a spori gradul de automatizare, conduce la creșterea gradului de expunere al sistemului informatic la atacuri cibernetice. Toate acestea realizându-se într-un context în care frecvența atacurilor cibernetice este in continuă creștere iar țintele devin din ce în ce mai diverse.

Sistemele de control industrial – Între performanță tehnologică și siguranță cibernetică

Conferința a fost deschisă de *Gratiela Magdalinoiu, Președinte al ISACA România*, urmată de o prezentare a cadrului actual legislativ susținută de domnul *Dragos Ichim, Expert în comunicare* pe zona securității cibernetice, Serviciul Român de Informații și de o scurtă prezentare a raportului EY privind statistica atacurilor cibernetice și a tendințelor din industrie. Acestea au precedat o sesiune de discuții sub formă de panel abordând contextul legislativ local și european privind protejarea infrastructurilor industriale, a riscurilor asociate din perspectiva guvernantei, a măsurilor de control, dar și a soluțiilor tehnice în raport cu amenințările curente.

Panelul a fost moderat de *Yugo Neumorni (fost Președinte ISACA România),* având ca invitați pe *Carmen Adamescu (Partner IT Advisory EY), Dragos Ichim (Expert în comunicare pe zona securității cibernetice SRI), Marian Raducu (Director IT&C al Transelectrica), Robert Stoicescu (Senior Manager Risk Assurance PwC).*

Reglementare – Provocări și planuri de implementare.

Un punct comun în cadrul discuției a venit din faptul că automatizarea este văzută ca un subiect insular, întrucât *sistemele legacy* sunt restricționate traficului în internet. Cu toate acestea, securitatea IT&C devine o componentă importantă în aceste sisteme industriale. Fiecare modernizare, care presupune un grad mai mare de automatizare, monitorizare și comandă de la distanță, prezintă noi provocări în menținerea nivelului de siguranță și securitate.

Cu toate acestea, vulnerabilitățile au început să fie vizibile, iar impactul major pe care îl poate avea un atac reușit, inerent. Suntem însă, atât la nivel european, cât și în România, într-o etapă incipientă, aceea de conștientizare, planificare și design. Un prim pas în această direcție este alinierea la Directiva Europeană 1148/2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (cunoscută și sub denumirea de Directiva NIS). Documentul prevede identificarea infrastructurilor critice la nivelul fiecărei țări din Uniune și adoptarea de planuri de prevenție și răspuns în cazul unui incident cibernetic.

Prevenția a fost un alt subiect discutat intens în cadrul panelului. Întrebări precum “Avem interoperabilitate la nivelul instituțiilor în caz de dezastru la un atac cibernetic?”, “Vom defini infrastructurile critice din România înainte sau după 2018?” sau “Ce abordare vom avea în implementarea măsurilor de securitate, unitară sau cazuala?“ au fost adresate și analizate de către invitați.

Deși din punct de vedere al legislației curente, infrastructura critică nu este clar definită, divizia CyberInt a Serviciului Român de Informații are o relație activă cu marile infrastructuri industriale și de utilități din România, existând o strategie națională ce include activități continue de monitorizare.

Reglementarea, din punct de vedere al formei, conținutului, incluzand detaliile si implicațiile cu care vine, este recomandat a fi discutată, agreată și dezvoltată în cadrul unor mese rotunde care să cuprindă experți din ambele zone (legislativă cât și tehnici), fiind necesar a rămâne într-o zona de prevenție, fără a ignora însă procedurile în caz de dezastru sau atac cibernetic.

Mai mult, a scrie despre legea securității cibernetice, a continua campania de conștientizare, a face demersuri cu implicare atât în zona publică cât și în domeniul privat, sunt acțiuni ce trebuie să continue într-un ritm susținut. Suportul factorilor de decizie din industrie precum și cel al reprezentanților instituțiilor publice responsabile, precum Ministerul Comunicațiilor și Societății Informaționale, este absolut necesar pentru a grăbi procesul de întocmire a propunerilor legislative.

Un prim pas în acest sens este alinierea la Directiva NIS până la finalul anului 2018, un cadru legislativ ce apare într-o piață cu multe provocări din perspectiva investițiilor în tehnologie și a limitărilor bugetelor asociate.

Evoluția tehnologică – security by design

Evoluția tehnologică a împins zona industrială către tehnologia IP, cea mai deschisă tehnologie la atacuri cibernetice. Astfel, apar o serie de întrebări privind adaptarea rețelelor la cele mai moderne echipamente. Ce se întâmplă cu soluțiile *end of support*? Cum putem să mitigăm riscurile cibernetice după o modernizare? Cum facem protocoalele de comunicație vechi și noi să coexiste?

Având în vedere oportunitățile ușor accesibile de a intra în sisteme digitale, segregarea și securizarea rețelelor devine una dintre cele mai importante măsuri, aceasta putând fi aplicată numai în cazul modernizărilor, așadar implică investiții. Totuși, trebuie remarcat faptul că o trecere mult prea rapidă către tehnologii de ultimă generație ar putea atrage un atac, cazurile deja cunoscute fiind cele în care investițiile nu au luat in calcul securitatea cibernetică, cum a fost cazul Ucrainei în decembrie 2015. O opțiune alternativă, dezbătuta pe parcursul discuțiilor, și în ton cu sintagma "grăbește-te încet" folosită de către unul dintre invitați, ar putea veni în urma implementării unei tehnologii intermediare in favoarea unui raport satisfăcător cost-beneficiu, din perspectiva vulnerabilităților.

Pe termen scurt, cu sau fără investiții în zona de securitate informatică, este recomandat însă a se implementa un set minim de măsuri de control cu un suport în sistemele de guvernanță și operare - standarde și proceduri de securitate minimale, care să acopere atât prevenția cât și intervenția în caz de incident.

Un alt aspect discutat în cadrul panelului a fost acela al vulnerabilităților echipamentelor și soluțiilor de ultimă generație, într-un context în care de multe ori consumatorul de tehnologie este mai atent la securitate decât producătorul. Astfel, devine datoria beneficiarilor finali de a fi vigilenți cu furnizorii de soluții și echipamente pentru a intra într-adevăr în mentalitatea security by design.

Nu în ultimul rând, a fost discutat pericolul atacurilor de tip social engineering: factorul uman este una din cele mai mari vulnerabilități a oricărui sistem informatic, independent de performanța acestuia. În acest context a fost subliniată nevoia de oameni calificați, specialiști în zona de control industrial, educați în spiritul securității informației, capabili să formeze operatorii de infrastructură, să ii auditeze și să formalizeze un cadru operațional care să susțină prevenția și capacitatea de răspuns în cadrul companiilor pe care le reprezintă.

Securitatea cibernetică în mediul industrial este la început de drum în România și în Europa în general. Astăzi, rolul părților implicate în acest spațiu este de a continua procesul de conștientizare, de a menține interesul și presiunea instituțională pentru propuneri legislative, de a implementa minimul necesar de securitate pe infrastructura existentă și de a forma o cultura a securității informatice în organizațiile din care fac parte. Având în vedere ritmul lent al formalizării cadrului legislativ, devine de datoria operatorilor să dezvolte ghiduri de bune practici pe specificul activităților lor și să asigure implementarea acestora.

"Security by design" a fost filozofia unanim acceptată de membrii panelului: furnizorii de echipamente, integratorii de tehnologie și operatorii de instalații, toți trebuie să fie aliniați la același ghid de securitate și bune practici în domeniu. Acest ghid trebuie sa fie testat, verificat și adaptat periodic reflectând vulnerabilitățile și amenințările actuale.

Security as a mindset – perspectiva tehnică

Ca o continuare a tuturor aspectelor discutate în panel, de data aceasta dintr-o perspectivă tehnică, *Sebastian Pitei (Director IT ENEVO Group)* a prezentat principalele vulnerabilități și măsuri de securitate ale echipamentelor și sistemelor de automatizare dintr-o rețea industrială, precum și soluțiile de Security Operation Center (SOC), soluții destinate monitorizării securității cibernetice a infrastructurilor industriale. Un accent deosebit a fost pus pe importanța formării capitalului uman, fie ca este vorba de angajați, contractori sau furnizori, întrucât fiecare din ei poate deveni o vulnerabilitate din perspectiva securității. Mai mult, deși o soluție SOC crește gradul de protecție a instalației, fără operatori bine pregătiți, capabili să ia decizii potrivite în baza alertelor platformei, *"Soluția"* nu va avea performanțele dorite.

Astfel, *"Security as a mindset"* vine în completarea principiului deja conturat în prima parte a conferinței, *"security by design",* și pune accent pe nevoia de resursă umană calificată pentru soluțiile tehnologice implementate sau viitoare.