Stimate Domnule Guvernator,

Stimate Domnule Prim-Vice Guvernator,

Stimați membri ai consiliului de Administrație al BNR,

Stimati oaspeți,

Este o onoare să fim împreună, astăzi.

Am sa incep prin a mulțumi conducerii BNR pentru încrederea acordată și sprijinul substanțial de care ne-am bucurat in organizarea acestui eveniment.

Mulțumim in mod deosebit Direcției de Audit Intern a BNR pentru aceasta excelenta inițiativa si pentru efortul depus in procesul de organizare, impreuna cu la colegii din Direcția Comunicare si Direcția Secretariat, si mai ales doamnei Director Maria Constantinescu care ne-a ajutat extrem de mult pe parcursul acestor săptămâni.

O mentiune speciala avem pentru unul dintre membii board-ului ISACA Romania, si trebuie sa va marturisesc ca suntem tare norocosi, care este in acelasi timp membru al echipei Direcției Buget si Analiza Financiara a BNR, doamna Dana Deaconu, care a asigurat, in detaliu, o cooperare si o comunicare foarte buna intre toate echipele implicate in organizare.

Le mulțumesc in egala măsura, colegilor din boardul ISACA, pentru efort, suport si perseverenta.

Va mulțumesc si dvs, tuturor celor prezenți pentru ca ne sunteti alături astazi.

###

Mi s-a intamlat sa spun, nu de putin ori, ca timpul sau lucrurile din jurul meu par sa alerge mai repede decat pot tine eu pasul. Si parca ritmul nu scade niciodata. Doar creste. Traim intr-o lume in continua schimbare iar tehnologia, internetul par ca urmeaza acest trend. Sau…poate e invers. Spatiul cibernetic este intr-o continua expansiune si asta are un impact considerabil asupra noastra ca indivizi, consumatori, dar si asupra mediului de afaceri privat si public. Probabil ambele afirmatii sunt adevarate in egala masura. Si se completeaza una pe cealalta.

Va invit mai departe sa aruncam o privire asupra unor detalii statistice.

Comsia Europeana, intr-un comunicat din octombrie 2017 spune ca:

- Anul trecut au avut loc zilnic peste 4 000 de atacuri de șantaj digital (ransomware);
- Asta inseamna o creștere de 300 % față de anul 2015;
- Impactul economic al criminalității cibernetice a crescut de cinci ori între 2013 și 2017 și se estimeaza o creștere de inca patru ori până în 2019;
- 80 % dintre organziatiile europene s-au confruntat cu cel puțin un incident legat de securitatea cibernetică;
- 87% dintre europeni sunt ingrijorati cu privire la criminalitatea cibernetica.

In noiembrie 2017 Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), a publicat un set de studii in care sumarizeaza proiectele europene deja implementate si rezultatele

acestora, in scopul selectarii unor piloni care pot deveni mai departe suport in promovarea cadrului legislativ existent si a politicilor de securitate cibernetica.

Concluziile scot in evidenta rezultate imbucuratoare in zone precum *usability, standardizare, acceptanta sociala, fiabilitate economica si conformitate.*

Bineinteles ca exista si observatii care scot in evidenta arii unde inca exista inca un numar mare de probleme nerezolvate de securitate cibernetica, privacy si trust care necesita eforturi de imbunatatire si corectie intr-o abordare holistica: tehnologie, componente, aplicatii si servicii.

Mergand spre zona de Internet of Things (IoT), considerata o paradigma in continua crestere cu implicatii tehnologice, sociale si economice, gasim atat riscuri si vulnerabilitati cunoscute dar bineinteles si multe noi, numarul acestora crescand exponential in timp. Adresarea acestora devine critica, si prioritara mai ales in contextul in care acestea vizeaza securitatea, intimitatea si siguranta indivizilor. In plus, acest ecosystem poate fi folosit ca vector de atatc si in infrastructuri critice (inclusiv sistemele de plati) - Intr-un context in care se estimeaza ca numarul de echipamente Internet of Things (IoT) vor atinge 20 miliarde pana in 2020.

Toate acestea sustin fara indoiala ideea digitalizarii. Si a faptului ca ea devine fundamentala pentru mediul economic si participantii acestuia. Bineinteles ca aduce multe oportunitati dar in acelasi timp vine cu un pachet generos de provocari.

Acesta este o imagine a momentului in care ne aflam.

Cu totii realizam ca exista progrese în ceea ce privește protejarea siguranței utilizatorului în mediul online, insa intelegem ca este inca mult loc pentru a imbunatati metodele, uneltele si sistemele existente.

Iar pentru asta avem nevoie de un cadru legislativ matur, o buna intelegere a profilelor de risc si a masurilor ce pot fi implementate pentru diminuarea acestora si bineinteles specialisti care sa sustina toate aceste procese.

Avem la nivel european initiative remarcabile care ne deschid oportunitati in acest sens:

- Strategia europeana pentru securitate cibernetica (revizuita la nivelul anului 2017) impreuna cu un sistem european de certificare cibernetica,
- Agenda digitala si Strategia pentru piata unica digitala,
- Directiva NIS (Directivei privind securitatea rețelelor și a informațiilor),
- GDPR (regulament privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal).

Ultimele 2 stim cu totii ca vor aduce multe provocari tinand cont ca ambele au termen de implementare in mai 2018.

Exista initiative deja in desfasurare si grupuri de lucru la nivel european pentru sustinerea implementarii acestor masuri. In plus, exista o propunere privind instituirea unei Agenții a UE pentru Securitate Cibernetică, construită pe bazele Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), cu rolul de a ajuta statele membre să prevină și să abordeze în mod eficace atacurile cibernetice, sa sustina punerea in aplicare a Directivei NIS (Directiva privind securitatea

rețelelor și a informațiilor) precum si sa acorde sprijin la instituirea și implementarea cadrului de certificare la nivelul UE (Cyber security Act).

Mai mult, anul acesta, ISACA a publicat pentru al treilea an consecutiv, rezultatele unui studiu la care au participat membri ai asociatiei din Europa, Asia si America de nord. Cateva rezultate interesante la nivel corporate:

- Atat numarul cat si pregatirea candidatilor pentru roluri de specialisti in securitate cibernetica este foarte scazut;
- Timpul mediu necesar pentru identificarea unui candidat cu profil potrivit este de 6 luni sau chiar mai mult;
- Mai mult de jumatate din participantii la sondaj au confirmat ca experienta si certificarile profesionale sunt cele mai importante criterii de selectie; - *asta poate iese*
- 50% din participantii la sondaj confirma ca bugetele alocate pentru anul urmator sunt in crestere, ceea ce inseamna insa o scadere cu 11% fata de anul anterior;
- In zona pozitiva avem si o crestere de 15 procente asociata includerii functiei de CISO in organigrama companiilor (de la 50% in 2016 la 65% in 2017).

Rezultatele subliniaza importanta componentei umane si implicarea in pregatirea specialistilor, si intelegem ca aceasta trebuie sa devina una din prioritatile organizatiilor, daca nu este deja.

Atat institutii guvernamentale precum si asociatii profesionale sunt deja angrenate in acest demers. Si aici as mentiona recenta propunere a Comisiei Europene de instituire a unui Centru european de cercetare și competență în materie de securitate cibernetică, un centru-pilot care ar urma să fie înființat în cursul anului 2018.

ISACA, a lansat in 2017 noua platforma de traininig pentru specialistii in securitate cibernetica, o spatiu unde cursantii au posibilitatea de a se antrena intr-un laborator live cu platforme si tehnologii diferite.

In plus, tot in 2017 asociatia a publicat materiale suport pentru auditul sistemelor de control din pespectiva securitatii cibernetice precum si pentru zona de data privacy.

Securitatea cibernetica este un subiect extrem de larg, care necesita o aprofundare minutioana, dar am increderea ca invitatii nostri va vor capta atentia cu detalii despre aspecte pe care le-am mentionat anterior: cadrul european si local, initiative si provocari, strategii, prioritati, roluri si responsabilitati.

Si am sa inchei cu un citat al domnului Profesor Doctor Udo Helmbrecht, Director executiv al ENISA care mi-a placut extrem de mult:

Cybersecurity is a shared responsibility. between technology companies, governments, and users.

Si aceste este si motivul pentru care ne aflam astazi aici.

Va multumesc pentru atentie.