

# CAPITAL

INVESTEȘTE ÎN INFORMAȚIE

18 august - 22 septembrie 2023 • Nr. 8 (1357) • 24,90 lei

## RETAILUL motorul străin de sub capota economiei românești

- Efectul X și lumea văzută prin ochii lui Musk
- Ce ne facem la iarnă cu gazul?

- Cine se luptă cu colmatarea Deltei? Nimeni! Deși există soluții. Și bani!

- Ce îi lipsește României pentru a deveni un hub logistic regional



# Ciprian Pocovnicu, TRU Solutions: «90% dintre amenințările informatice vin prin e-mail»

Pe măsură ce apar noi oportunități de business odată cu Revoluția Digitală, și riscurile pe care și le asumă companiile sunt din ce în ce mai mari și mai complexe. Securitatea digitală de nivel înalt, mai ales pentru companiile din servicii esențiale, care trebuie să se conformeze cu directivele NIS1 și NIS2 ale UE, devine o preocupare intensă.

**P**entru Capital, am discutat cu Ciprian Pocovnicu, expert în securitate cibernetică cu peste 20 de ani de experiență și fondator al TRU Solutions, despre îmbunătățirea măsurilor de securitate, dar și despre colaborarea cu autoritățile naționale și adaptarea la schimbările legislative.

„Directiva NIS reprezintă un set de norme stabilite de Uniunea Europeană, cu scopul de a îmbunătăți securitatea cibernetică în statele membre. Acestea se aplică companiilor operatoare de servicii esențiale din sectoarele de sănătate, energie, transport, financiar, bancar, utilități și servicii digitale”, spune pentru Capital Ciprian Pocovnicu.

Conform expertului în securitate cibernetică, principalele direcții pe care companiile trebuie să le urmeze pentru a fi conforme normelor directivei NIS sunt:

- ✓ Protecția împotriva amenințărilor cibernetice (să se implementeze măsuri tehnice pentru a proteja confidențialitatea informațiilor și a se proteja împotriva amenințărilor cibernetice).

- ✓ Politici de securitate cibernetică (companiile trebuie să definească politici clare și detaliate care acoperă toate aspectele securității cibernetice, inclusiv protecția datelor, accesul la rețea, utilizarea programelor).

- ✓ Planuri de răspuns la incidente (în cazul unui incident de securitate cibernetică, trebuie să existe planuri de răspuns ce vor încerca să limiteze daunele).



- ✓ Gestionarea riscurilor (trebuie să se efectueze evaluări periodice de risc pentru a identifica și a remedia orice vulnerabilitate).

- ✓ Raportare (trebuie să se raporteze orice incident de securitate la autoritatea națională competentă).

- ✓ Recuperare după incident (companiile trebuie să definească planuri de recuperare pentru a se asigura că pot reveni rapid la operațiunile normale după un incident de securitate cibernetică).

### Există riscuri mari

„Am implementat normele directivei NIS în companii medii și mari din România, din industriile de sănătate, transport și energie. Măsurile impuse sunt similare, indiferent de industria în care își desfășoară activitatea compania operatoare de servicii esențiale. Însă majoritatea companiilor cu care am colaborat nu aveau implementate sisteme de criptare a datelor în stocare cu posibilitatea gestionării cheilor de criptare, cerință explicită NIS”, ne spune Pocovnicu.

E adevărat, sistemele de e-mail și de stocare a documentelor tradiționale criptează

informațiile doar în tranzit, stocarea fiind realizată „în clar”, expunându-se astfel riscurilor care privesc confidențialitatea și securitatea datelor. În acest caz, ce se poate face?

„Primul pas în conformarea cu normele directivei NIS este implementarea suitei de confidențialitate și securitate a datelor, Proton Business, care include e-mail, stocare de fișiere, VPN și calendar, ușor de utilizat, cu stocare criptată în Elveția. Ulterior, în funcție de etapa de dezvoltare a securității informatice a companiei, am dezvoltat strategia de implementare a măsurilor și soluțiilor necesare conformării”, declară expertul în cibersecuritate.

Care sunt amenințările cibernetice în prezent

„Aproape 90% din amenințările informatice la adresa companiilor ajung prin e-mail, fiind cel mai utilizat canal pentru schimbul de informații cu exteriorul. Cele mai mari amenințări sunt reprezentate de phishing - mesaje frauduloase prin care se încearcă obținerea de informații confidențiale sau instalarea de malware pe dispozitivele victimei, ransomware - programe care criptează datele utilizatorului și solicită o răscumpărare pentru a le debloca sau malware - programe malițioase, cum ar fi virușii, troienii și viermii, care pot provoca daune sistemelor și rețelelor informatice”, ne informează fondatorul TRU Solutions.

„Proton Mail utilizează o echipă de savanți dedicată și tehnologii proprii pentru a preveni atacurile informatice:

Eliminarea elementelor de tracking, care pot transmite expeditorului informații personale: nume, adresa IP, locația geografică, statutul mesajului șamd. Alte pericole la care sunt expuse companiile sunt reprezentate de furtul de identitate, exploatarea vulnerabilităților software, atacuri de tip „man-in-the-middle”, infracțiuni interne sau atacuri de tip ddos”, subliniază Pocovnicu.

Lacunele de securitate și depășirea lor

Din perspectiva normelor directivei NIS, Ciprian Pocovnicu spune că lacunele pe care le-a identificat în companiile de servicii esențiale cu care a colaborat nu sunt deloc puține. Iată principalele greșeli: neconsiderarea soluției de e-mail fiind esențială; necriptarea datelor companiei; necunoașterea amenințărilor cibernetice actuale (amenințările cibernetice evoluează rapid, atât în complexitate cât și în diversitate); lipsa unor politici și proceduri clare de securitate cibernetică (se neglijează necesitatea politicilor de securitate bine definite și actualizate); lipsa unei culturi de securitate cibernetică; (angajații pot deveni cea mai slabă verigă și pot cădea pradă atacurilor de phishing); gestiunea

Ce sunt NIS 1 și NIS 2

Directiva NIS reprezintă un set de norme stabilite de Uniunea Europeană, cu scopul de a îmbunătăți securitatea cibernetică în statele membre. Acestea se aplică companiilor operatoare de servicii esențiale din sectoarele de sănătate, energie, transport, financiar, bancar, utilități și servicii digitale.

Directiva NIS 2, privind securitatea cibernetică pentru protejarea infrastructurilor critice și digitale, a intrat în vigoare la nivel european începutul anului 2023, extinzând lista sectoarelor și a activităților vizate. Spre deosebire de Directiva NIS, care prevedea 7 sectoare esențiale, Directiva NIS2 propune o nouă abordare, respectiv 11 sectoare esențiale: Energie; Transport; Sectorul bancar; Infrastructuri ale pieței financiare; Sectorul sănătății; Apă potabilă; Ape uzate; Infrastructură digitală; Gestionarea serviciilor TIC; Administrație publică; Spațiu și 7 sectoare importante: Servicii poștale și de curierat; Gestionarea deșeurilor; Fabricarea, producția și distribuția de substanțe chimice; Producția, prelucrarea și distribuția de alimente; Fabricarea de dispozitive medicale, a computerelor și a produselor electronice și optice, a echipamentelor electrice, a autovehiculelor, remorcilor și semiremorcilor; Furnizori digitali; Cercetare. Directiva NIS 2 se va transpune național în România până cel târziu la data de 17 octombrie 2024.

inadecvată a accesului (accesul necontrolat sau neautorizat la resursele informatice creează lacune de securitate semnificative); lipsa testării și planificării în caz de incidente de securitate; lipsa actualizărilor și patch-urilor (asta expune sistemele informatice vulnerabile la atacuri).

„Proton Mail și Proton Drive folosesc criptare end-to-end, de nivel militar, pentru a securiza e-mailurile și documentele atât în tranzit, cât și în stocare. Utilizatorul dispune de o cheie de criptare proprie, unică și gestionabilă. Funcție de nivelul de securitate ales, autentificarea se poate face cu o parolă de acces, o parolă pentru decriptarea datelor, cu o cheie software sau cu o cheie hardware. Dacă parola de acces a conținutului ar fi interceptată, sau în cazul improprie în care ar fi sustrate date din serverele Proton, atacatorul nu va putea accesa conținutul acestora, fiind criptate”, ne explică expertul Pocovnicu. I

