TUCA ZBARCEA
ASOCIATII

14 aprilie 2020

COVID-19 Ştiri Legislative

În acest număr:

1. **Asigurarea securității cibernetice a sistemelor de prelucrare a datelor cu caracter personal în contextul lucrului de la distanță**

Recomandări privind securitatea cibernetică pentru angajatorii care implementează sisteme de lucru la distanță

EUROPOL a declarat recent faptul că numărul de atacuri cibernetice împotriva organizațiilor și a persoanelor fizice a crescut semnificativ în contextul COVID-19. Informațiile de mai jos sunt furnizate în lumina opiniilor recent exprimate la nivelul autorităților de reglementare europene și al Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA).

1. **Ce măsuri de control pot lua angajatorii pentru protejarea informațiilor acestora în contextul lucrului de la distanță?**

În vederea protejării informației în contextul în care salariații lucrează de la distanță, angajatorii pot adopta o serie de măsuri la nivel organizațional, precum și măsuri de ordin tehnic, după cum urmează:

a) Măsuri organizaționale:

- Să furnizeze angajaților în mod regulat informații despre cum ar trebui să acționeze în cazul în care întâmpină dificultăți în utilizarea instrumentelor de lucru la distanță (e.g. personal autorizat pe care îl pot apela, orele de lucru, proceduri în caz de urgență).
- Să asigure asistență în caz de probleme întâmpinate de angajați în utilizarea instrumentelor de lucru la distanță. Acest lucru poate necesita stabilirea unui program special pentru personal.
- Să interzică accesul la internet de pe protocoalele de acces la distanță (sau alte protocoale potențial vulnerabile) atunci când nu este necesar.
- Să se asigure că angajații cunosc pe deplin procedurile de acces la distanță (de ex. VPN, autentificare multi-factor etc.).
- Să se asigure că toți angajații pot fi contactați în orice moment și că aceștia sunt familiarizați cu mijloacele de contactare.

- Să restricționeze accesul la sisteme care necesită o protecție specială. De exemplu, sistemul de management al conectivității angajaților va putea fi accesat doar de personal IT dedicat, intranetul și sistemele de pontaj vor putea fi accesate doar de manageri etc.
- Să instituie o procedură de autorizare prealabilă a utilizării dispozitivelor personale ale angajatului (BYOD).

b) Măsuri tehnice

- Să ofere angajaților accesul de la distanță doar printr-o soluție de tip VPN sau altă soluție cu caracteristici similare.
- Să implementeze soluții virtuale sigure de certificare digitală, cum ar fi semnătura electronică extinsă, fluxuri de aprobare virtuală etc.
- Să asigure efectuarea periodică a copiilor de rezervă a tuturor fișierelor importante.
- Să implementeze soluții IT adecvate pentru a contracara acțiunile frauduloase ale hackerilor care ar încerca să exploateze situația generată de lucrul la distanță, inclusiv prin propagarea *ransomware* și utilizarea unor tehnici de *phishing* având ca pretext știri despre Covid-19.
- Să se asigure că infrastructura IT pentru accesul la distanță are suficientă capacitate și licențe pentru a acoperi numărul crescut de utilizatori care necesită acces simultan, inclusiv prin testarea capacității rețelei.
- Să se asigure că actualizarea automată a stațiilor de lucru ale angajaților se realizează și atunci când angajații lucrează de acasă.
- Să reamintească angajaților să efectueze în mod regulat actualizarea stațiilor de lucru, a software-ului de securitate și a altor instrumente de securitate (cum ar fi *add-on*-uri pentru browsere).

2. Ce recomandări pot face angajatorii personalului care lucrează de acasă?

- Să folosească doar instrumentele și canalele de comunicare pe care organizația le pune la dispoziție și să amintească periodic angajaților faptul că politicile de securitate se aplică și atunci când aceștia lucrează de acasă (e.g. regulile de utilizare a conturilor de e-mail private și a serviciilor de schimb de fișiere).
- Să folosească, pe cât posibil, rețele de date mobile 4G sau 5G, întrucât acestea asigură o protecție adecvată a informațiilor din și către dispozitivul folosit.
- Să folosească doar o conexiune Wi-Fi sigură, pentru a împiedica interceptarea și accesarea datelor de către persoane neautorizate.
- Să asigure securitatea accesului fizic la computerul lucru, cum ar fi să blocheze ecranul atunci când nu lucrează.

- Să fie precauți cu privire la orice mesaj electronic prin care li se solicită să verifice sau, după caz, să-și reînnoiască credențialele, să acceseze diverse link-uri sau să transmită diverse informații/ documente, chiar dacă mesajul pare să provină dintr-o sursă de încredere. Să încurajeze angajații să verifice autenticitatea cererii prin orice alte mijloace.

ciprian.timofte@tuca.ro

florentina.petrisor@tuca.ro

Editori

Știri Legislative - COVID-19 reprezintă răspunsul nostru în contextul epidemiei de coronavirus din România. Firma noastră a constituit un grup de lucru dedicat gestionării implicațiilor juridice născute în contextul răspândirii COVID-19. Avocați din departamentele de conformare/ reglementare, drept societar și comercial, asigurări, dreptul muncii, litigii și arbitraje, insolvență, achiziții publice, protecția datelor cu caracter personal, precum și consultanți specializați în domeniul fiscal și vamal vin în întâmpinarea clienților cu sfaturi și asistență pe subiecte specifice situațiilor de criză economică: restructurări, analiza și (re)negocierea contractelor (inclusiv a celor colective și individuale de muncă), executarea contractelor afectate de forță majoră și impreviziune, deblocarea raporturilor pre-litigioase etc. Pentru a fi la curent cu noutățile în acest domeniu, puteți accesa resursele disponibile la următorul link: *http://www.tuca.ro/covid-19/*

Ciprian Timofte
Partner
+4 0374 136 341
ciprian.timofte@tuca.ro

TUCA ZBARCEA ASOCIATII

Șos. Nicolae Titulescu nr. 4-8
America House, Aripa de Vest, et. 8
Sector 1, 011141, București, România
T + 4 021 204 88 90
F + 4 021 204 88 99
E office@tuca.ro
www.tuca.ro