DNSC: Activitatea companiei care detine brandul Cocorico, afectata sever de un atac ransomware

Directoratul National de Securitate Cibernetica (DNSC) a fost notificat, duminica, 9 martie, în legatura cu atacul cibernetic desfasurat asupra AAylex One, grupul integrat din industria alimentara, care include fluxul complet de productie, distributie si comercializare a produselor din carne de pui, cunoscute sub marca Cocorico, a informat institutia într-un comunicat de presa transmis, joi, AGERPRES.

"În cel mai scurt timp, specialistii DNSC s-au deplasat la fata locului pentru a oferi suport în remedierea incidentului. În acest moment, o investigatie ampla este în desfasurare, informatiile preliminare indicând ca este vorba despre un atac informatic de tip ransomware lansat de un grup infractional international. Activitatea companiei a fost sever afectata, urmând ca aceasta sa fie reluata progresiv, pe masura ce activitatile de investigatie si remediere sunt derulate, cu sprijinul partenerilor specializati în domeniul securitatii cibernetice si cu asistenta expertilor DNSC. AAylex a luat masurile care se impun pentru informarea partilor-cheie interesate, precum si pentru diminuarea impactului asupra activitatilor proprii si partenere. Mentinerea comunicarii constante reprezinta una dintre principalele prioritati ale companiei, astfel încât se bazeaza pe colaborarea si întelegerea tuturor partenerilor sai, în perioada de timp necesara pentru depasirea acestor dificultati si pâna la revenirea completa a activitatii grupului, conform standardelor de calitate si excelenta obisnuite", precizeaza Directoratul.

Specialistii în securitatea cibernetica din cadrul DNSC recomanda tuturor partenerilor companiei sa fie vigilenti si sa trateze cu atentie sporita orice mesaje suspecte primite în numele AAylex, precum si sa evite furnizarea de date confidentiale specifice, prin canale nesecurizate, "întrucât momentan nu exista acces la adresele de email si canalele de comunicare oficiale cunoscute".

Alte recomandari de urmat în astfel de cazuri fac referire la implementarea unor masuri de securitate cibernetica cu caracter general, precum: sporirea vigilentei la verificarea e-mailurilor primite, în special a celor care contin atasamente sau linkuri suspecte; utilizarea unei solutii de tip anti-malware care sa permita scanarea automata a atasamentelor si linkurilor; actualizarea de urgenta a sistemelor de operare, a programelor antivirus, browserelor web, clientilor de e-mail si a programelor de tip Office; monitorizarea continua a accesului la retea de catre cei responsabili din departamentele IT; instalarea unei solutii de control al aplicatiilor; crearea unor puncte de restaurare a sistemului si realizarea de back-up pentru fisiere; realizarea periodica de sesiuni de training cu personalul.