SRI ia în calcul cinci scenarii cu posibile atacuri cibernetice în timpul alegerilor

Specialistii Centrului National Cyberint, din cadrul Serviciului Român de Informatii, au elaborat cinci scenarii în cazul unor posibile atacuri cibernetice asupra sistemelor informatice folosite de institutiile publice în perioada alegerilor europarlamentare si prezidentiale din acest an.

Specialistii sustin ca, în timpul desfasurarii scrutinelor electorale din acest an, exista posibilitatea ca actori externi cu relevanta geostrategica sa influenteze procesul electoral prin utilizarea unor capabilitati cibernetice.

Autoritatea Electorala Permanenta este institutia care se ocupa de gestionarea alegerilor din România, iar sistemele informatice utilizate la alegeri sunt dezvoltate de AEP, Serviciul de Telecomunicatii Speciale, dar si companii private de IT.

Preocuparea specialistilor români vine dupa ce, în ultimii ani, grupari rusesti au lansat atacuri cibernetice pentru a influenta rezultatul alegerilor din Ucraina (gruparea de hackeri CyberBerkut a compromis si blocat în anul 2014 sistemul informatic al Comisiei Centrale de Alegeri), Marea Britanie (campanii agresive pro-Brexit prin utilizarea unor sisteme de "boti" de catre organizatia ruseasca Internet Research Agency), SUA (atacuri cibernetice din Rusia si denigrarea candidatului Hillary Clinton), Franta (publicarea de documente false în timpul alegerilor prezidentiale din 2017), Germania (atac cibernetic în anul 2015, care a vizat Parlamentul si birourile cancelarului Angela Merkel).

Pe baza experientei statelor care s-au confruntat cu atacuri cibernetice, specialistii Cyberint au elaborat cinci scenarii cu privire la interferenta unor actori externi în alegeri.

* *Infectarea sistemelor IT&C utilizate în cadrul procesului electoral*, prin atacuri cibernetice asupra Registrului Electoral Central si asupra sistemelor informatice folosite la centralizarea si numararea voturilor. Un asemenea atac cibernetic ar afecta integritatea listelor de alegatori, ar altera partial rezultatul alegerilor si ar aduce prejudicii de imagine pe plan intern si extern.

* *Interceptarea comunicatiilor existente între misiunile diplomatice ale României si AEP* prin atacuri cibernetice. În acest caz ar fi afectata integritatea datelor (prin modificarea numarului votantilor) transmise de misiunile diplomatice catre AEP si ar duce la indisponibilizarea canalelor de comunicatii utilizate de misiunile diplomatice.

* *Operatiuni de propaganda si dezinformare* - prin crearea de conturi false pe platformele de socializare si transmiterea de informatii false (fake-news) catre un numar cât mai mare de persoane. Aceste operatiuni pot favoriza un anumit candidat si denigra un contracandidat, prin propagarea de stiri false cu ajutorul "trolilor".

* *Distribuirea de documente cu caracter confidential* obtinute ca urmare a unor atacuri cibernetice.

* *Atacuri cibernetice asupra infrastructurilor IT&C* ale unor trusturi media românesti.

Specialistii Cyberint au mai multe recomandari pentru a preveni atacurile cibernetice în timpul alegerilor: testarea riguroasa a sistemelor informatice utilizate în procesul electoral, utilizarea de solutii de back-up la intervale cât mai scurte de timp, derularea unor campanii de constientizare la nivelul opiniei publice cu privire la riscurile asociate campaniilor de propaganda si dezinformare.