

Newsletterul „Unde tragem linia” revine cu câteva ediții speciale, în care îți vom aduce o serie de ghiduri practice despre cum să gestionezi mai bine unele probleme de securitate ce-ți pot afecta organizația, dar și bunăstarea jurnaliștilor. În ediția de astăzi, navigăm alături de Mykola Kostynyan, consultant în securitate digitală, printre **tipurile de hărțuire cibernetică la care pot fi supuși jurnaliștii** și cum se pot transforma acestea în riscuri de securitate.



Mykola Kostynyan

consultant în securitate digitală

În teoria securității, riscul e un eveniment nedorit care îți cauzează probleme reale și care îți poate afecta misiunea și scopul. Multe dintre riscurile provocate intenționat de către cineva, mai ales repetate constant, se simt ca o formă de hărțuire pentru jurnaliști. Am selectat câteva exemple ce s-au întâmplat în perioada electorală jurnaliștilor din Moldova și le-am cuplat cu câteva sfaturi.

Dar mai întâi de toate, **cum putem deosebi un risc real de „gălăgia online”?**

Riscul are doi parametri importanți: probabilitatea și impactul. În funcție de acestea, doar organizația poate decide cât de mare este un risc pentru sine. Dacă un anumit risc ne face imposibilă activitatea, atunci acesta este unul mare. Prin urmare, ce e real și ce e „gălăgie” decidem doar noi. Dacă ne afectează operațiunile, atunci e ceva real, dacă putem trăi cu asta, atunci s-ar putea să-i amânăm rezolvarea. Din acest motiv, este util să facem o evaluare de riscuri. Spre finalul newsletterului, vei găsi câteva sfaturi despre când și cum putem să o facem.

Cazul 1. Ce facem dacă ne trezim cu paginile de Social Media clonate?

Când ni se întâmplă ceva pe platformele sociale, primul lucru pe care îl putem face este să raportăm problema pe platforma respectivă prin mecanismele interne de raportare. Ar fi bine ca în spațiul dedicat unei explicații să insistăm cu detalii despre faptul că suntem o organizație media și că merităm mai multă atenție în acest caz, așa cum importanța noastră în societate este mare. Pe lângă aceasta, o idee bună ar fi să apelăm la ajutorul organizației [Access Now](#). Organizația are contacte directe cu platformele mari și ne poate accelera cazul.

Preventiv, ar fi de ajutor să avem insigne de verificare ale meta, pentru ca utilizatorii să le fie mai ușor să facă distincția între conținutul fals și cel real. De asemenea, putem încuraja audiența să raporteze paginile false.

În acest caz, riscul e atât reputațional, cât și de scurgere de date, dacă conținutul fals reușesc să ceară cuiva informații confidențiale sau documente din numele organizației.

Clonarea ar putea să vizeze și paginile personale ale jurnaliștilor, pentru care urmăm aceiași pași.

Cazul 2. Ce facem dacă ne este clonată pagina web?

În cazul website-ului, în primul rând atragem atenția la numele domain-ului. Administratorul site-ului, în cazul în care există acest rol în redacție, poate căuta numele domain-ului și găsi registratorul acestuia. Apoi, următoarea etapă este identificarea companiei de găzduire web. S-ar putea să nu aflăm asta, dar am putea identifica faptul că website-ul clonă folosește serviciul de Cloudflare, spre exemplu. Pentru următoarea etapă, ar fi bine să avem un avocat care să ne ajute să elaborăm o solicitare de suspendare a activității site-ului respectiv pe motiv de abuz și violarea drepturilor de autor. Scrisoarea o putem transmite celor de la Cloudflare sau companiei de găzduire web. Chiar dacă nu vor reuși să-l suspende, cel puțin ar putea să-l includă într-o listă neagră, ca atunci când e accesat, utilizatorii să primească o notificare că website-ul e suspicios.

Dacă nu există capacitate internă, putem să apelăm la Acces Now sau la oricare asistență de securitate. Și în acest caz riscul este reputațional, însă s-ar putea ca aceste clone să distribuie anumiți viruși pentru a infecta computerele celor care le accesează.

Pentru ambele cazuri, e important să comunicăm audienței despre aceste probleme pe canalele oficiale deținute.

Cazul 3. Ce facem dacă primim e-mailuri de la conturi care copiază identitatea autorităților sau altor organizații oficiale?

Acesta este un caz de atac cibernetic concret — phishing. De regulă, într-un astfel de atac va trebui să facem o acțiune, să accesăm un link, să descărcăm ceva, să deschidem un fișier în computer. Printr-un atac de phishing poate fi preluat controlul la e-mail, la Google Drive, poate fi infectat calculatorul cu viruși. Și dacă la această etapă, aceste e-mailuri sunt simplu de depistat, trebuie să înțelegem că această formă de atac devine din ce în ce mai sofisticată. Phishing-ul este extrem de periculos, ne așteptăm să existe tot mai multe astfel de cazuri în regiune.

Acest atac implică în egală măsură aspecte psihologice și tehnice. Ca să luptăm cu aspectul tehnic trebuie să ne protejăm conturile în moduri în care phishing-ul nu ar funcționa, adică să avem activată autentificarea prin factori multipli, inclusiv cu o cheie de securitate. Autentificarea în doar doi pași nu este rezistentă la phishing. La fel de importantă este educarea membrilor echipei la fiecare jumătate de an, cu oferirea de exemple proaspete, cu discuții despre acestea și explicarea semnelor de suspiciune. Dacă ai resurse limitate, dar vrei să organizezi un training de securitate în organizația ta, atunci acesta trebuie să fie despre phishing, pentru că se poate întâmpla nu doar pe e-mail, dar și pe Signal, WhatsApp, Telegram și alte servicii de mesagerie.

Suspiciunea trebuie să apară când primim un mesaj emoțional care ne sperie cu ceva, ne oferă ceva, de exemplu — o informație exclusivă pentru o investigație. Oamenii din redacție trebuie să știe cum să procedeze dacă primesc astfel de mesaje. În primul rând, nu ar trebui să interacționeze cu expeditorul, dar să arate cuiva din redacție acest mesaj, în mod ideal unei persoane care are mai multe cunoștințe în acest domeniu. Nu putem să antrenăm în totalitate oamenii să distingă mesajele reale de cele false, dar putem să-i antrenăm să distingă mesajele suspicioase. Dacă cuiva din redacție i s-a întâmplat un astfel de caz, acesta trebuie discutat cu toată echipa, pentru că probabilitatea ca și colegii să primească mesaje similare este mare.

O măsură preventivă ar fi ca toată lumea să aibă acces la ultimele versiuni de Windows/Mac/iOS/Android. Toate aplicațiile trebuie să fie actualizate, iar utilizarea programelor nelicențiate să fie evitată. O idee bună ar fi un antivirus corporativ cu un panou de control centralizat, prin care o persoană desemnată poate monitoriza în timp real problemele de securitate ale computerelor organizației.

Cazul 3.1. Ce facem dacă cineva a preluat controlul conturilor sociale sau e-mailurilor?

Preluarea poate avea loc doar prin phishing. Dacă e-mailul poate fi securizat prin autentificare cu mai mulți pași, inclusiv cu o cheie de securitate, și prin activarea Google Advanced Protection, atunci mesajele nu pot fi protejate cu o cheie de securitate. Pentru acestea e necesar să avem măcar autentificarea cu doi factori și să educăm oamenii prin exemple. Dacă preluarea a avut loc, putem și în acest caz să apelăm la ajutorul organizației [Access Now](#).

Care e cea mai vulnerabilă platformă?

Platforma de comunicare pentru echipă trebuie să fie comodă pentru ritmul de lucru. Alegem platforma în funcție de scopuri, apoi ne asigurăm că o protejăm. Pentru Slack, de exemplu, e o idee bună să avem un sistem centralizat corporativ, pentru care să facem o înregistrare unică. Astfel, membrii echipei nu vor trebui să-și facă parole și login separat, dar să se conecteze cu contul Google, care ar putea fi protejat prin autentificare cu factori multipli.

Cea mai vulnerabilă platformă e cea care conține cele mai importante informații pe care vrem să le protejăm.

Cazul 4. Ce facem cu atacurile coordonate din partea trollilor pe rețelele sociale?

Raportăm activitatea trollilor acolo unde e posibil, pentru că în unele cazuri, platforma le poate descoperi și închide rețeaua. Activitatea trollilor nu reprezintă un risc imediat, dar aceștia ar putea să-și dezvolte rețelele, să capete anumite abilități, să înțeleagă istoricul interacțiunilor de pe contul nostru, să facă raportări masive, care ne pot afecta vizibilitatea, iar aici vorbim deja despre un atac direct la operațiunile organizației. Ar trebui să fim atenți la semnele de căderi bruște de interacțiuni, vizualizări etc.

Bonus. Cum facem o evaluare de riscuri?

Evaluarea riscurilor e primul pas pentru a gestiona riscurile într-o organizație. Aceasta cuprinde toate tipurile de securitate și e făcută de echipa de management, chiar dacă ar putea fi facilitată și de consultanți externi. Managementul însă trebuie să ia deciziile. Vom începe mai întâi cu definirea și înțelegerea a ceea ce vrem să protejăm.

Evaluarea va avea loc anual, iar în urma acesteia trebuie să obținem o listă de riscuri în ordine prioritară de rezolvare. Gestionarea riscurilor poate include acțiuni precum prevenire, reducere, evitare, acceptare, transferare și altele.

Apoi vom dezvolta un plan de implementare a măsurilor pe care le-am ales. Odată ce implementăm planul, putem spune că deja am început să îmbunătățim măsurile de securitate relevante pentru noi în acea perioadă de timp. Urmează un proces de monitorizare, evaluare și anumite corecturi necesare, ca să înțelegem dacă planul nostru lucrează.



Oportunitate!

1. **Google Workspace pentru organizațiile non-profit** este deja disponibil în Moldova. Opțiunea îți oferă posibilitatea să crezi un sistem corporativ de e-mailuri, prin care să poți controla securitatea conturilor de e-mail ale membrilor echipei. Poți să decizi ce măsuri de securitate să activezi pentru acestea, poți controla accesul și opțiunile de distribuire de pe Google Drive. [Verifică opțiunea aici](#).

2. Asociația Presei Independente pune la dispoziție un **serviciu de consultanță pentru redacțiile regionale și naționale independente** din țară, care se confruntă cu riscuri de securitate cibernetică și alte probleme legate de protecția informațiilor și securitatea online. Vezi [aici](#) detalii.



Cere ajutor!

Dacă te confrunți cu stres constant și anxietate, poți solicita o consultație gratuită și confidențială cu un psiholog prin intermediul [acestui chatbot](#) sau completează [acest formular](#). Vei fi pus(ă) în legătură cu un specialist în decurs de 48 de ore.

Dacă ți-a plăcut ce ai citit, recomandă newsletterul nostru unui coleg/colega de breaslă. Feedbackul ne va ajuta să devenim mai buni. Scrie-ne ce crezi despre newsletter la adresa api@api.md.



Acest newsletter a fost produs cu suportul financiar al Uniunii Europene. Conținutul acestuia reprezintă responsabilitatea exclusivă a proiectului
„TRIMEDIA – Jurnalism de încredere, media de impact, comunități implicate”,
 FINANȚAT DE Uniunea Europeană și cofinanțat de Ministerul Federal German pentru Cooperare Economică și Dezvoltare (BMZ). Conținutul materialului aparține autorilor și nu reflectă în mod neapărat viziunea Uniunii Europene.