

Zeci de pagini cu informații tehnice și termeni greu de înțeles, uitate într-un dosar ascuns în cel mai îndepărtat colț al dulapului. Nu, aceasta nu e politica de securitate pe care să o adopți în organizația ta și nu despre un astfel de document vom vorbi în ediția de astăzi. Împreună cu Joseph Hamood, manager de securitate și riscuri în cadrul International Media Support, **îți explicăm cum se face o politică de securitate simplă, aplicabilă și eficientă pentru redacția ta.**

Joseph Hamood

expert de securitate și riscuri,
International Media Support



Cum introducem conceptul de securitate echipei noastre fără a crea panică?

Trebuie să explicăm echipei că securitatea e necesară pentru a ne continua operațiunile în orice situație, iar pentru asta e nevoie să înțelegem care sunt acele lucruri care ne-ar împiedica continuitatea. E foarte important să conectăm riscurile și securitatea cu continuitatea afacerii, pentru că acesta e de fapt motivul pentru care dezvoltăm o astfel de politică. Documentul trebuie să ne spună pe care amenințări să ne focalizăm atenția și cum să le rezolvăm.

Cum se face o politică de securitate?

Cel mai mare risc al unei politici de securitate este să fie prea lungă și greu de înțeles. Angajarea cuiva care să producă un document doar pentru a-l ține pe raft și a-l arăta ocazional donatorilor nu rezolvă problema. **O politică de securitate ar trebui să fie un instrument util și practic**, nu o formalitate birocratică. Nu mărimea politicii e importantă, ci faptul că e a noastră. O putem ajusta oricând, pe măsură ce organizația evoluează. Monitorizarea și revizuirea politicii poate fi un exercițiu anual de echipă.

Pentru început, ne vom aduna cu întreaga echipă și vom identifica lucrurile care ne amenință munca și posibilitatea de a ne continua operațiunile. Este important ca aceste riscuri să reflecte realitatea noastră, nu presupunerile unor persoane externe. Această discuție trebuie să fie sinceră și să descopere ce ne îngrijorează cu adevărat. Pot fi aspecte de management, conflicte interne, atacuri externe, situația politică, probleme legale. Chiar dacă unele dintre ele sunt sensibile, trebuie să le conștientizăm și să le abordăm, altfel vor continua să crească și, într-o zi, pot genera o criză.

După ce știm ce ne poate afecta munca, le punem într-o ordine în funcție de urgența cu care trebuie abordate. Apoi căutăm soluțiile potrivite pentru fiecare, astfel încât să le putem gestiona eficient.

Următorul pas e să identificăm alte părți interesate. Oricare ar fi problemele descoperite, nu suntem singuri în asta. Trebuie să înțelegem ce aliați avem și care e rolul jucat de ei. În continuare, e important să stabilim o relație cu aceștia, să discutăm cu ei înainte de o eventuală criză.

E necesar să luăm în considerare și aspectele etice și morale așa cum sunt obligația de a avea grijă, incluziunea de gen — lucruri pe care s-ar fi putut să le ignorăm la început. Apoi, ne vom concentra pe elaborarea unui plan de rezervă pentru cele mai urgente riscuri.

Cel mai important aspect al acestui proces este că reprezintă munca echipei, ceea ce face atât procesul, cât și rezultatele mult mai relevante. Sunt ideile noastre despre cum să ne protejăm organizația, iar în acest fel politica devine una practică și ancorată în realitate.

Rolul politicii este să ne pregătească din timp pentru potențialele amenințări, deoarece doar prin pregătire putem asigura continuitatea organizației.

Când e momentul potrivit să lucrăm la politica noastră de securitate?

În mod cert, trebuie să facem asta atunci când lucrurile sunt calme. Planificarea se face înainte de criză, nu ne putem pregăti în timp ce luptăm, pentru că astfel doar vom reacționa, însă esența pregătirii este să putem răspunde proactiv.

Avem nevoie de un ghid în realizarea politicii?

Da, aveți nevoie de un ghid, însă nu de un expert care să ne facă politica în locul nostru sau să ne ofere un formular tipizat pe care să-l copiem. În procesul de analiză a riscurilor se discută cinci aspecte importante: operațional, politic, legal, financiar și reputațional. Echipa va discuta fiecare dintre aceste domenii, însă persoana care ghidează conversația poate oferi direcție sau feedback.

Cine face parte din echipa de gestionare a unei crize?

Când alegem echipa de gestionare a unei crize, este important să selectăm persoane care cunosc bine organizația și procesele interne, indiferent de funcția pe care o dețin. Avem nevoie și de persoane tehnice, iar aici contrazicem punctul de vedere de mai sus, pentru că în acest caz nu e necesar ca experții IT, spre exemplu, să fie parte din organizație. Ei ne pot ajuta cu o sarcină specifică și nu e nevoie să facă parte din echipa de management a crizei.

La fel și pentru partea de consultanță generală în situații de urgență, putem apela la un expert extern. Asta nu înseamnă că echipa de criză devine mai mare, ea va fi formată în continuare din persoanele de bază din organizație, doar că vom avea și câteva contacte adiționale pe care le putem activa la necesitate.

Echipa de criză se creează după analiza și evaluarea riscurilor pe baza concluziilor și necesităților identificate, pentru că doar la acea etapă vom înțelege de câți oameni avem nevoie și la ce persoane din extern trebuie să apelăm.

Ce se întâmplă după o criză?

După criză analizăm ce s-a întâmplat, ce putea fi făcut mai bine, ce s-a dovedit util în practică, ce instrumente am folosit și în ce mod, cum trebuie să actualizăm politica noastră. Întotdeauna vom găsi goluri, pentru că crizele sunt dinamice. Indiferent cât suntem de pregătiți, vor exista zone oarbe.

Cât de multă informație de criză trebuie să primească angajații, colaboratorii și publicul nostru?

În echipă există managerii care gestionează criza și există oamenii afectați de ea. Trebuie să înțelegem cine poate fi afectat și cum să ne adaptăm comunicarea în funcție de fiecare grup.

Membrilor de echipă care nu sunt implicați în gestionarea crizei, dar care sunt afectați direct, trebuie să le comunicăm aspectele relevante pentru a putea lua decizii. De exemplu, dacă are loc un atac cibernetic sau un raid al biroului, echipa trebuie informată să stea acasă. Trebuie să aplicăm o strategie de comunicare pentru echipă, ca să primească actualizări regulate (zilnic, o dată la două zile sau mai rar, în funcție de situație). Publicul, în schimb, nu trebuie informat la fiecare două zile. Poate fi suficient și un anunț public despre ce s-a întâmplat, cum ne afectează, ce servicii se schimbă etc.

De aceea, un pas important în analiza riscurilor este și analiza partenerilor implicați în raport cu riscurile.

Cum să bugetăm corect pentru ca să putem răspunde prompt la necesitățile de securitate?

În acest moment vorbim despre modul în care siguranța și pregătirea de criză se intersectează cu dezvoltarea organizațională. Toate planurile pentru asigurarea continuității operaționale trebuie să facă parte din bugetul de dezvoltare.

Aici un rol important îl vor juca partenerii organizației, cărora trebuie să le comunicăm că astfel investim în securitatea organizației și în continuitatea dezvoltării noastre. De exemplu, atunci când dezvoltăm infrastructura IT, asta nu ne oferă doar protecție, asta înseamnă că investim de fapt în reziliența și capacitatea organizației. Nu e doar o problemă de securitate, dar e o necesitate de dezvoltare organizațională.

În situațiile de criză reală, va exista un sprijin suplimentar de la diferiți actori, iar dacă avem deja planurile și știm exact de ce avem nevoie, vom putea reacționa rapid cu cerințe precise.

Deci, pe de o parte avem bugetul de dezvoltare, iar pe de altă parte avem situații de urgență, pentru care vom accesa fonduri de urgență.



Oportunitate!

Redacțiile pot obține granturi pentru dezvoltarea capacităților instituționale. Printre activitățile eligibile se numără inițiativele de întărire a securității digitale, precum și cele dedicate prevenirii burnout-ului și susținerii sănătății mintale a echipelor editoriale. Află [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/collega de breaslă. Feedbackul ne va ajuta să devenim mai buni. Scrie-ne ce crezi despre newsletter la adresa api@api.md.