orange™ Business

CargoTrack™

Cum răspunzi unui incident cibernetic

De la un atac DDoS asupra CargoTrack la monitorizare și răspuns continuu prin MDR

CargoTrack

operațiuni protejate, reziliență crescută

Ce se întâmplă atunci când un atac cibernetic limitează accesul clienților la o platformă importantă pentru activitatea lor zilnică?

Într-un astfel de moment, presiunea nu este resimțită doar de echipa IT. Efectele ajung rapid la clienți, la echipele de suport și la operațiunile companiei. În paralel, fiecare modificare realizată pentru restabilirea serviciilor trebuie analizată atent, pentru a nu crea vulnerabilități noi.

CargoTrack s-a confruntat cu un atac DDoS care a afectat accesul clienților la platforma digitală folosită pentru administrarea flotelor. Echipa internă a aplicat primele măsuri tehnice, iar atunci când atacul s-a intensificat, Orange Business a mobilizat specialiștii SCUT și a facilitat colaborarea dintre echipele implicate.

În mai puțin de 30 de minute de la escaladarea situației, a fost stabilit un plan comun de răspuns. Partea critică a incidentului a fost stabilizată în aproximativ două ore, fără compromiterea datelor companiei sau ale clienților.

Incidentul nu a fost tratat ca un episod încheiat odată cu restabilirea accesului. CargoTrack a continuat cu testarea infrastructurii, extinderea măsurilor de Disaster Recovery, inventarierea dependențelor tehnologice și dezvoltarea monitorizării continue prin Managed Detection & Response.

orange™ Business

CargoTrack™

CargoTrack în cifre, la momentul atacului

16.000+
clienți activi

~50.000
camioane conectate în Europa la momentul atacului

16
servere în infrastructură, dintre care unul sau două vizate mai intens

< 30 de minute
pentru mobilizarea echipelor și stabilirea planului comun

~2h
pentru stabilizarea părții critice a incidentului

0
date ale companiei sau ale clienților compromise

CargoTrack este o companie românească specializată în soluții pentru managementul flotelor și plata automată a taxelor de drum. Compania are o echipă de 65 de persoane, iar serviciile sale sunt utilizate de transportatori din România și din alte țări europene.

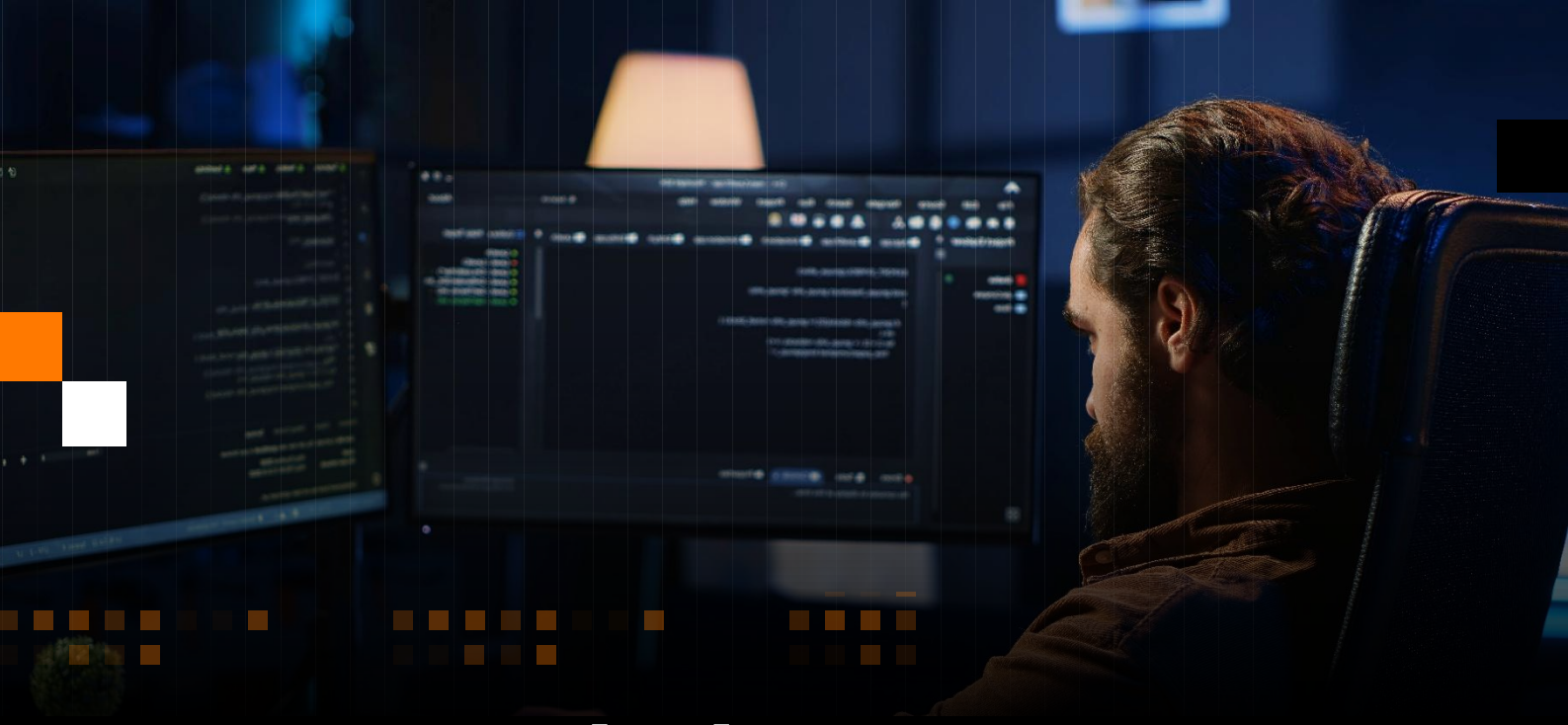
Platforma CargoTrack, esențială pentru clienți

Clienții folosesc platforma digitală CargoTrack pentru a monitoriza vehiculele, a administra flotele și a gestiona conturile necesare plății taxelor de drum.

În acest context, indisponibilitatea platformei nu reprezintă doar o problemă IT. Dacă nu se pot autentifica, clienții nu mai au acces la informațiile necesare pentru coordonarea flotelor, iar efectele pot ajunge rapid la dispeceri, șoferi, echipele de suport și operațiunile desfășurate în mai multe țări.

La momentul incidentului, aproximativ 50.000 de camioane utilizau serviciile CargoTrack în Europa. Atacul a perturbat accesul clienților la platforma de management, însă componenta dedicată plății taxelor de drum era izolată și a rămas funcțională.

> **Pentru noi, instabilitatea serviciilor contează foarte mult. Nu ne permitem să avem perioade în care platforma nu poate fi accesată. În momentul în care un client nu mai poate intra în platformă, nu mai vede unde sunt mașinile și nu își mai poate gestiona activitatea.**
> Răzvan Perțicaș, Fondator CargoTrack



Aspecte cheie ale răspunsului CargoTrack la atac

Atacul a început prin episoade sporadice de trafic anormal, care au afectat treptat funcționarea platformei CargoTrack.
Ulterior, traficul s-a intensificat și s-a concentrat asupra unuia sau a două servere dintr-o infrastructură formată din 16 servere.

Cum funcționează un atac DDoS

Un atac DDoS, Distributed Denial of Service, generează un volum foarte mare de trafic către un website, o aplicație sau un server. Resursele disponibile sunt suprasolicitate, iar utilizatorii legitimi nu mai pot accesa serviciul sau îl pot utiliza doar cu dificultate.
În cazul CargoTrack, impactul atacului s-a concentrat asupra disponibilității platformei. Datele companiei și ale clienților nu au fost compromise.

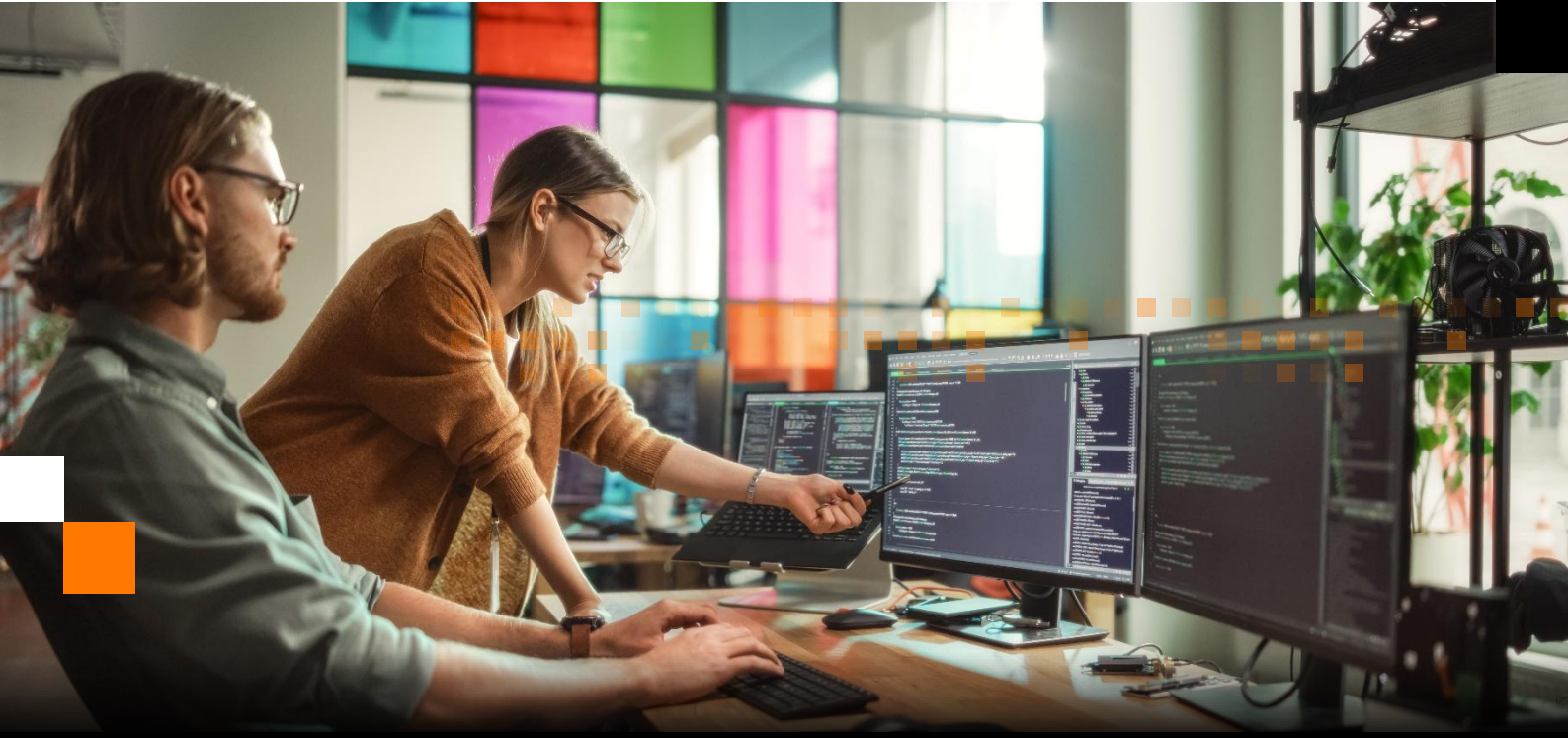
Ce impact a avut asupra platformei?

Pe măsură ce atacul s-a intensificat:

- clienții au întâmpinat dificultăți la accesarea platformei;
- informațiile necesare administrării flotelor nu mai puteau fi consultate în condiții normale;
- echipa CargoTrack a primit într-un interval scurt mii de apeluri;
- presiunea asupra echipelor tehnice și de suport a crescut rapid.

Atacul nu a compromis datele CargoTrack sau ale clienților.

Componenta dedicată plății taxelor de drum era izolată și a rămas funcțională. Incidentul a afectat accesul la platformă, dar nu a fost o breșă de date.



Primele măsuri luate de echipa CargoTrack

Echipa tehnică CargoTrack a identificat degradarea serviciului și a încercat să limiteze impactul prin blocarea anumitor tipuri de acces și prin redirecționarea traficului între servere.

Aceste măsuri au contribuit la gestionarea primelor episoade ale atacului. Odată cu intensificarea traficului, intervențiile au devenit însă mai complexe. În timpul unui incident, presiunea de a restabili rapid serviciile poate determina echipele să aplice mai multe modificări într-un interval scurt. Fără o coordonare clară, acestea pot crea vulnerabilități noi sau pot face mai dificilă înțelegerea efectului fiecărei acțiuni. Principala preocupare a CargoTrack nu mai era doar limitarea atacului. Echipa trebuia să păstreze controlul asupra schimbărilor aplicate în infrastructură.

> **Colegii mei îmi spuneau că se descurcă, dar am vrut să mă asigur că nu ne creăm singuri vulnerabilități prin modificările pe care le făceam. În timpul unui atac, lucrurile se precipită foarte repede și există riscul să greșești.**
> Răzvan Perțicaș, Fondator CargoTrack

Momentul escaladării către Orange Business

CargoTrack a contactat Orange Business în afara programului obișnuit, în momentul în care atacul s-a intensificat și a crescut riscul unor intervenții necontrolate în infrastructură.

În mai puțin de 30 de minute, Orange Business a organizat un apel comun la care au participat:

- echipa CargoTrack;
- reprezentanții Orange Business;
- specialiștii SCUT;
- ceilalți parteneri tehnici relevanți pentru infrastructura companiei.

Pregătirea documentelor necesare și mobilizarea resurselor tehnice s-au desfășurat în paralel. Prioritatea a fost înțelegerea situației și stabilirea rapidă a unui plan comun de răspuns.

Orange Business a facilitat legătura dintre echipa clientului, partenerii tehnici și specialiștii în securitate necesari pentru gestionarea incidentului.

> **Când am văzut apelul lui Răzvan, am înțeles că situația se complicase. Am început să-mi sun colegii și am ajuns rapid la Ciprian și la echipa SCUT. Toți și-au arătat disponibilitatea: o echipă pregătea documentele, în timp ce alta se pregătea pentru intervenție.”**
> **Florin Cormoș, Business Development Executive, Orange Business**

Cum a fost stabilit planul comun de răspuns

Înainte de aplicarea altor modificări, echipele au analizat situația și au stabilit un plan comun. Planul a clarificat:

- cine răspunde pentru fiecare acțiune;
- ce sisteme și servere trebuie verificate;
- ce modificări pot fi aplicate;
- cine validează schimbările;
- ce efecte trebuie monitorizate;
- cum sunt comunicate rezultatele între echipe.

Specialiștii SCUT au urmărit în timp real intervențiile realizate în infrastructură.

Obiectivul nu era doar restabilirea accesului. Fiecare măsură trebuia aplicată controlat, astfel încât intervenția să nu expună alte sisteme și să nu creeze vulnerabilități noi.

> **În maximum jumătate de oră eram în apel cu toată echipa. Am stabilit un plan și l-am aplicat. Colegii de la SCUT monitorizau fiecare mișcare făcută în infrastructură, iar după aproximativ două ore am reușit să stabilizăm lucrurile.**
> **Răzvan Perțicaș, Fondator CargoTrack**

De ce expertiza umană contează în timpul unui incident

Tehnologia poate identifica anomalii și poate genera alerte. Totuși, deciziile trebuie luate în funcție de infrastructura companiei, de serviciile afectate și de impactul asupra operațiunilor.

În timpul incidentului CargoTrack, specialiștii SCUT au urmărit acțiunile aplicate de echipa tehnică și au contribuit la păstrarea unui ritm controlat al intervenției.

Diferența dintre un instrument care generează alerte și un serviciu gestionat constă în capacitatea specialiștilor de a verifica informațiile, de a înțelege contextul și de a susține alegerea măsurilor potrivite.

> **Toată lumea era tensionată, însă colegul SCUT care lucra direct asupra situației avea un calm ieșit din comun. Analiza fiecare pas și spunea clar ce trebuie făcut. În acele momente s-au văzut experiența și profesionalismul echipei.”**
> Florin Cormoș, Business Development Executive, Orange Business

Cum a fost stabilizată partea critică a incidentului?

Răspunsul a fost organizat în trei etape:

1. Aplicarea planului comun
Echipele au aplicat măsurile agreate și au monitorizat efectele fiecărei schimbări realizate în infrastructură.
Fiecare acțiune a avut un rol clar, iar modificările au fost urmărite pentru ca restabilirea accesului să nu creeze riscuri noi.

2. Stabilizarea în aproximativ două ore
Partea critică a incidentului a fost stabilizată în aceeași seară.
Accesul la serviciile afectate a fost readus în parametri funcționali, fără compromiterea datelor companiei sau ale clienților.

3. Continuarea măsurilor în ziua următoare
Intervenția nu s-a încheiat odată cu stabilizarea platformei.
Începând din ziua următoare, CargoTrack, Orange Business și SCUT au continuat analiza infrastructurii și au accelerat măsurile necesare consolidării securității.

De la intervenția punctuală, la monitorizare continuă

Incidentul a confirmat că răspunsul eficient nu depinde de o singură soluție. Contează colaborarea dintre echipa internă, partenerii tehnologici și specialiștii în securitate.

O bază de securitate deja existentă

Înaintea atacului, CargoTrack avea o echipă internă implicată în securitate și începuse discuțiile cu Orange Business și SCUT privind consolidarea protecției infrastructurii.
Acest nivel de pregătire a permis companiei să identifice situația, să aplice primele măsuri și să solicite sprijin înainte ca modificările realizate sub presiune să creeze riscuri suplimentare.

Un răspuns coordonat între echipe

În timpul incidentului, echipa CargoTrack, Orange Business, specialiștii SCUT și ceilalți parteneri tehnici au lucrat după un plan comun, cu acțiuni monitorizate și responsabilități clare.

Trecerea către monitorizare permanentă

Experiența a accelerat extinderea serviciului Managed Detection & Response și trecerea către un model bazat pe:

- **monitorizare de securitate 24/7;**
- **analizarea și validarea alertelor;**
- **identificarea evenimentelor relevante;**
- **acces la specialiști;**
- **răspuns coordonat la incidente.**

> **Un incident bine gestionat nu înseamnă finalul drumului. Înseamnă începutul unei etape mai mature de securitate.**
>
> Ciprian Foghiș, Senior ICT Business Development Manager, Orange Business

orange Business

CargoTrack™

Ce este Managed Detection & Response

Managed Detection & Response, prescurtat MDR, este un serviciu care combină tehnologia de detectare cu analiza și intervenția specialiștilor. Serviciul urmărește permanent evenimentele de securitate din infrastructura companiei, corelează informațiile și ajută la identificarea alertelor care necesită intervenție.
MDR nu înlocuiește echipa internă. Îi oferă vizibilitate suplimentară, monitorizare în afara programului și acces la specialiști care pot analiza evenimentele în context.

> **Managed Detection & Response înseamnă monitorizare activă non-stop și răspuns imediat. Nu este doar o soluție software care trimite alerte. Specialiștii verifică ce se întâmplă și intervin atunci când este nevoie.**
>
> Ciprian Foghiș, Senior ICT Business Development Manager, Orange Business

Ce asigură Managed Detection & Response

Monitorizare 24/7: urmărește permanent evenimentele de securitate din endpointuri, servere, rețea și servicii cloud.
Corelarea alertelor: reunește semnalele provenite din mai multe sisteme pentru a identifica evenimentele care necesită atenție.
Validare realizată de specialiști: analiștii verifică alertele în context și reduc volumul notificărilor care nu indică un incident real.
Răspuns coordonat la incidente: ajută la prioritizarea acțiunilor și susține echipele în aplicarea măsurilor necesare.
Raportare și recomandări: oferă vizibilitate asupra incidentelor și recomandări pentru consolidarea nivelului de securitate.

Cum se completează MDR cu protecția împotriva atacurilor DDoS

Managed Detection & Response și protecția DDoS au roluri diferite, dar complementare.
MDR asigură monitorizarea continuă, analizarea alertelor și răspunsul coordonat, în timp ce măsurile complementare protejează rețeaua, aplicațiile și continuitatea serviciilor.
Împreună, acestea contribuie la construirea unei protecții pe mai multe niveluri.

Măsuri care completează MDR

Protecție dedicată DDoS
Identifică și filtrează traficul anormal înainte ca acesta să afecteze disponibilitatea serviciilor.

Protecția rețelei și aplicațiilor
Reduce expunerea infrastructurii și a serviciilor accesibile din internet.

Managementul vulnerabilităților
Identifică, evaluează și prioritizează punctele slabe care trebuie remediate.

Teste de penetrare și de stres
Verifică rezistența infrastructurii și a aplicațiilor în scenarii controlate.

Backup și Disaster Recovery
Susțin recuperarea sistemelor și continuarea activității atunci când serviciile sunt afectate.

Ce a schimbat CargoTrack după incident

CargoTrack nu a tratat atacul ca pe un episod încheiat odată cu restabilirea accesului. Incidentul a accelerat un plan de securitate aflat deja în dezvoltare și a adus mai rapid în prim-plan măsurile necesare pentru consolidarea infrastructurii.

Testarea infrastructurii

CargoTrack a continuat cu teste de penetrare, teste de stres și verificări suplimentare.

Obiectivul a fost validarea măsurilor existente și identificarea zonelor în care nivelul de protecție putea fi consolidat.

Extinderea măsurilor de Disaster Recovery

Compania avea deja o soluție de Disaster Recovery.

După incident, a analizat opțiuni suplimentare pentru recuperarea sistemelor și reducerea dependenței de o singură configurație.

Inventarierea dependențelor tehnologice

Analiza a fost extinsă de la sistemele proprii la:

- furnizorii tehnologici;
- API-urile utilizate;
- serviciile externe;
- adresele IP;
- conexiunile dintre aplicații și sisteme.

Astfel, CargoTrack a obținut o imagine mai clară asupra suprafeței de atac și a riscurilor din întregul ecosistem digital.

Extinderea monitorizării

Monitorizarea a fost extinsă la nivelul calculatoarelor și serverelor.

Alertele sunt analizate atât de echipa internă, cât și de specialiștii SCUT, pentru ca evenimentele relevante să poată fi identificate și tratate mai rapid.

Accelerarea investițiilor în securitate

Pentru 2026, CargoTrack a alocat aproximativ 200.000 de euro buget pentru securitate cibernetică în ansamblu.

Bugetele planificate pentru întregul an au fost activate mai rapid, pentru a susține testarea, monitorizarea și măsurile suplimentare de reziliență.

> **Partea importantă este că cineva monitorizează activ. Nu este doar un software care îți trimite o alertă și te lasă să decizi singur ce s-a întâmplat. Cineva verifică, iar dacă este ceva important, te contactează.**
> Răzvan Perțicaș, Fondator CargoTrack

Un parcurs în șase pași pentru răspuns și consolidare

Experiența CargoTrack arată că răspunsul la un incident începe înainte ca acesta să se producă și continuă după restabilirea serviciilor. Cele șase acțiuni de mai jos formează un parcurs de la pregătire la consolidarea rezilienței.

Stabilește echipa și partenerii

Clarifică din timp cine răspunde pentru securitate, cine ia deciziile și ce parteneri pot fi contactați atunci când apare un incident.
Datele de contact, rolurile și modalitatea de escaladare trebuie să fie cunoscute înainte de apariția unei situații critice.

Pregătește un plan de răspuns

Definește responsabilitățile, pașii de escaladare și modul în care sunt aprobate și monitorizate modificările realizate în infrastructură.
Un plan existent ajută echipa să acționeze mai rapid și reduce riscul deciziilor contradictorii.

Analizează alertele în context

Verifică dacă semnalele primite indică un incident real și prioritizează acțiunile în funcție de impactul asupra serviciilor.
Nu toate alertele au același nivel de risc. Contextul operațional ajută la stabilirea ordinii corecte a intervențiilor.

Coordonează echipa internă cu specialiștii MDR

Echipa companiei oferă contextul infrastructurii și al operațiunilor.
Specialiștii MDR adaugă monitorizare continuă, analiză și experiență în gestionarea incidentelor.

Evaluează întregul ecosistem digital

Include în analiză serverele, aplicațiile, furnizorii, API-urile și serviciile cloud care pot extinde suprafața de atac.
Securitatea nu se oprește la infrastructura aflată direct în administrarea companiei.

Transformă securitatea într-o prioritate de business

Folosește concluziile incidentului pentru a îmbunătăți continuitatea serviciilor, investițiile și capacitatea companiei de a răspunde pe viitor.
Securitatea influențează experiența clienților, operațiunile, reputația și capacitatea companiei de a-și respecta promisiunile comerciale.

Checklist pentru evaluarea capacității de răspuns

Întrebările de mai jos sunt construite pornind de la experiența CargoTrack. Ele pot ajuta o companie să identifice ce trebuie clarificat înainte, în timpul și după un incident.

Înaintea unui incident

- Știm ce servicii trebuie să rămână disponibile permanent?
- Avem inventariate serverele, aplicațiile și serviciile cloud?
- Cunoaștem API-urile și furnizorii de care depinde infrastructura?
- Este clar cine ia deciziile în timpul unui incident?
- Știm cine poate fi contactat în afara programului?
- Avem un plan de escaladare?
- Alertele sunt monitorizate 24/7?
- Avem o soluție de Disaster Recovery testată?
- Am realizat recent teste de penetrare sau de stres?

În timpul unui incident

- Am stabilit un singur punct de coordonare?
- Este clar cine execută fiecare acțiune?
- Fiecare modificare este validată înainte de aplicare?
- Monitorizăm efectele fiecărei intervenții?
- Separăm serviciile afectate de sistemele care trebuie protejate?
- Evităm aplicarea simultană a unor modificări necoordonate?
- Documentăm deciziile și rezultatele?
- Managementul primește informațiile necesare pentru luarea deciziilor?

.

După stabilizarea incidentului

- Am verificat dacă datele sau sistemele au fost compromise?
- Am analizat ce a funcționat și ce trebuie schimbat?
- Retestăm infrastructura după aplicarea măsurilor?
- Revizuim furnizorii și dependențele externe?
- Actualizăm planul de răspuns?
- Verificăm soluțiile de backup și Disaster Recovery?
- Extindem monitorizarea acolo unde există zone fără vizibilitate?
- Informăm managementul asupra riscurilor și investițiilor necesare?

Întrebări pentru management

Un incident cibernetic nu este doar un subiect tehnic. Pentru a înțelege nivelul real de pregătire, managementul ar trebui să poată răspunde la câteva întrebări simple.

- Cât timp poate funcționa compania dacă o aplicație importantă nu mai este disponibilă?
- Ce servicii generează cel mai mare impact operațional dacă sunt întrerupte?
- Cine monitorizează alertele în afara programului?
- Cât de repede poate fi mobilizată o echipă de răspuns?
- Cine poate aproba modificări urgente în infrastructură?
- Sunt cunoscute toate dependențele față de furnizori și servicii externe?
- Când au fost testate ultima dată procedurile de recuperare?
- Cum este informat managementul în timpul unui incident?
- Ce buget este disponibil pentru prevenție, monitorizare și răspuns?
- Cum este măsurat progresul programului de securitate?

Răspunsurile neclare indică zone care trebuie analizate înainte de apariția unui incident.

Securitatea cibernetică, o decizie pentru întregul business

> **Securitatea este unul dintre acele lucruri importante care nu par urgente. Dar, când devin urgente, poate fi deja prea târziu dacă nu te-ai pregătit. Probabil că nu ești niciodată suficient de pregătit, dar este important să ai un plan.**
>
> Răzvan Perțicaș, Fondator CargoTrack

Experiența CargoTrack arată că securitatea nu poate rămâne doar în responsabilitatea departamentului IT. Disponibilitatea platformei influențează direct clienții, operațiunile și echipele de suport. În același timp, deciziile privind monitorizarea, testarea, Disaster Recovery și bugetele necesită implicarea managementului.

Concluzie

CargoTrack s-a confruntat cu un incident cibernetic, dar a avut capacitatea de a identifica problema, de a aplica primele măsuri și de a solicita sprijin înainte ca presiunea să determine modificări necontrolate în infrastructură.
Orange Business a mobilizat specialiștii și a facilitat coordonarea, iar echipa SCUT a urmărit intervențiile și a susținut luarea deciziilor tehnice.
Partea critică a incidentului a fost stabilizată în aproximativ două ore. Datele companiei și ale clienților nu au fost compromise, iar componenta dedicată taxării a rămas funcțională.
Experiența a devenit apoi punctul de plecare pentru accelerarea unui program mai amplu de securitate: testarea infrastructurii, extinderea măsurilor de Disaster Recovery, inventarierea dependențelor tehnologice și monitorizarea continuă prin Managed Detection & Response.
Concluzia nu este că o singură tehnologie poate opri orice atac. Un răspuns eficient se bazează pe:

- echipe pregătite;
- responsabilități clare;
- monitorizare continuă;
- intervenții coordonate;
- acces la specialiști;
- măsuri complementare de protecție;
- implicarea managementului.

Securitatea cibernetică este un proces continuu, construit înaintea incidentului și îmbunătățit după fiecare test real al infrastructurii.

Știi ce se întâmplă.

Reacționezi la timp.

Managed Detection & Response este serviciul SCUT disponibil prin Orange Business, care combină monitorizarea de securitate 24/7, tehnologii avansate de detecție și analiza specialiștilor în securitate cibernetică.

Ce obține compania ta:

- Vizibilitate asupra evenimentelor relevante de securitate
- Corelarea alertelor din mai multe sisteme și surse
- Reducerea alertelor nerelevante și a zgomotului operațional
- Identificarea rapidă a incidentelor care necesită intervenție
- Sprijin pentru coordonarea răspunsului la incidente
- Rapoarte și recomandări pentru consolidarea posturii de securitate

Programează o discuție despre Managed Detection & Response pe orange.ro/business/securitate-cibernetica/

orange™ Business