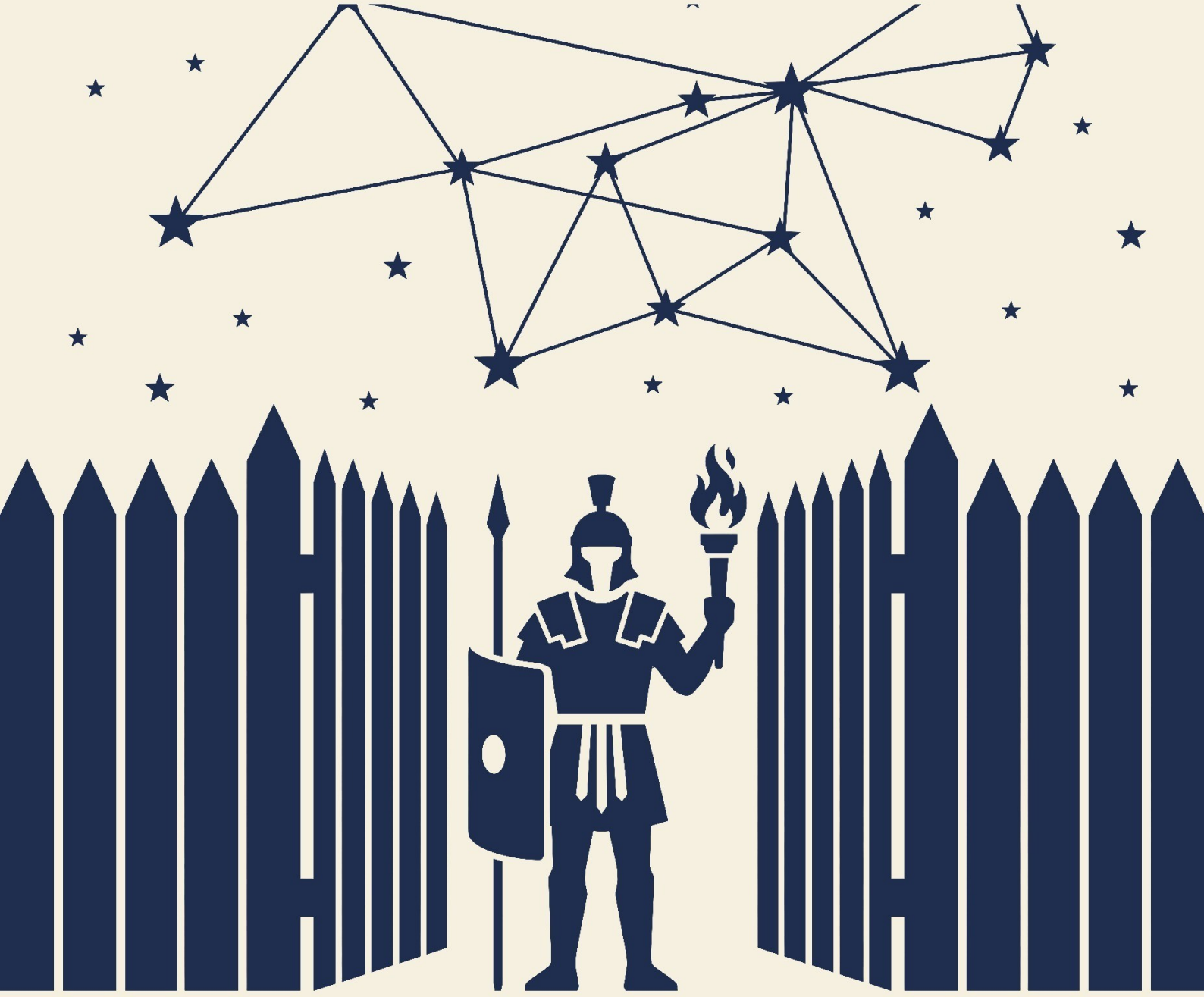
SECURITATE VECHE PENTRU AMENINȚĂRI NOI

Tehnici dinaintea internetului care încă funcționează

12 fișe practice, de la legiunile romane la deepfake · GDPR · NIS2 · ISO 27001



Dan Gurghian

gurghian.ro · 2026

Cuprins

Introducere: de ce funcționează încă metodele vechi 3

1 Parola de recunoaștere 6

2 Regula celor doi 10

3 Runbook-ul pe hârtie 14

4 Sigiliul 18

5 Copia de la mănăstire 22

6 Compartimentarea 26

7 Chirograful 30

8 Mesagerul și spațiul gol 34

9 Blocul de unică folosință (one-time pad) 38

10 Momeala 42

11 Codul de constrângere 46

12 Jurnalul santinelei 50

Plan de acțiune: prima zi, prima săptămână, prima lună 54

Mituri: unde „vechiul” nu te salvează 57

Tabel de corelare: tehnici și obligații legale 61

Bibliografie adnotată 63

Despre autor 66

Introducere: de ce funcționează încă metodele vechi



Un director de la Ferrari a oprit, în vara lui 2024, o fraudă construită cu cea mai nouă tehnologie disponibilă — o voce clonată de inteligența artificială — cu o tehnică pe care legionarii romani o foloseau la poarta taberei: o întrebare la care doar persoana reală putea răspunde. Nu a avut nevoie de un program, de un abonament sau de un consultant. A avut nevoie să știe că tehnica există.

Această carte pleacă de la o observație simplă: amenințările cibernetice sunt noi, dar problemele pe care le pun nu sunt. Cum verifici că cel care îți vorbește este cine spune că este? Cum împiedici un singur om să fure tot? Cum păstrezi un secret care trebuie, totuși, să rămână accesibil? Cum știi dacă cineva a umblat la un document? Cum te asiguri că paznicul chiar a stat de pază? Oamenii au răspuns la aceste întrebări timp de câteva mii de ani, în condiții în care greșeala costa orașe, armate și vieți, iar răspunsurile lor au fost testate cu o brutalitate pe care niciun audit de securitate nu o poate reproduce.

Majoritatea acestor răspunsuri nu depind de tehnologie. Depind de structură: cine știe ce, cine poate face ce, cine verifică pe cine, ce se întâmplă când ceva lipsește. Tocmai de aceea rămân valabile. Un firewall este bun până la următoarea vulnerabilitate; regula că niciun om nu poate muta singur banii din seif este bună de cinci sute de ani și va fi bună și când seiful va fi un portofel de criptomonede.

Ce nu este această carte

Nu este o carte despre istorie, deși conține multă. Fiecare poveste de aici este verificabilă și are o sursă, dar este spusă pentru ceea ce învață, nu pentru farmecul ei.

Nu este o pledoarie pentru întoarcerea la hârtie și la mașina de scris. Capitolul de mituri, de la sfârșit, explică de ce o asemenea întoarcere este, de cele mai multe ori, o iluzie — și uneori o greșeală mai gravă decât problema pe care încearcă s-o rezolve. Tehnicile vechi nu înlocuiesc măsurile moderne. Le completează acolo unde măsurile moderne au un punct orb: omul.

Nu este nici o colecție de metafore. „Firewall-ul este ca zidul unui castel" este o comparație plăcută și inutilă. Fișele de aici se opresc la ce se poate face luni dimineață, cu pași concreți, pentru o firmă de 20 de oameni și pentru una de 500.

Cum sunt construite fișele

Fiecare dintre cele douăsprezece tehnici este prezentată după aceeași structură, ca să poată fi citită în orice ordine și folosită ca referință. Fișa începe cu tehnica într-o frază, adică ce este și contra cui funcționează, și continuă cu originea ei, cu sursa istorică. Urmează principiul, invariantul de securitate pe care îl exploatează și numele sub care este cunoscut azi, apoi amenințarea de azi, un caz real și recent în care lipsa tehnicii a costat sau prezența ei a salvat.

Partea practică se numește „Cum o implementezi luni dimineață" și dă pași concreți pe două dimensiuni de organizație, plus, unde are sens, varianta pentru acasă. Partea cea mai importantă se numește „Unde eșuează" și descrie limitele, modurile de abuz și motivele pentru care tehnica a picat istoric — o carte despre securitate care nu spune unde eșuează fiecare măsură nu este o carte despre securitate. Fișa se încheie cu cadrul legal, adică obligația din GDPR, din Directiva NIS2 și din ISO/IEC 27001:2022 pe care tehnica o acoperă, astfel încât un responsabil cu protecția datelor, un auditor sau un director să o poată cita direct în documentația de conformitate. Trimiterile dintre fișe sunt în text, acolo unde o tehnică se sprijină pe alta, pentru că aproape niciuna nu funcționează singură.

Trei etichete, la începutul fiecărei fișe, spun epoca din care vine tehnica, amenințarea actuală pe care o acoperă și costul implementării. Veți observa că la majoritatea costul este zero. Nu este o coincidență. Cele mai bune măsuri de securitate inventate vreodată au fost inventate de oameni care nu aveau buget.

O precizare, ca să nu fie nevoie de ea la fiecare pagină. Tehnicile de aici completează măsurile tehnice moderne — autentificarea cu mai mulți factori, actualizările, protecția endpoint-urilor —, nu le înlocuiesc, iar documentarea lor este un punct de plecare pentru conformitate, nu o dovadă a ei. Ce obligații aveți și ce măsuri sunt adecvate depinde de riscurile concrete ale organizației voastre, pe care nicio carte nu le poate evalua în locul vostru.

Cui îi este adresată

Directorilor de firme mici și mijlocii, care nu au departament de securitate și nici nu vor avea. Administratorilor IT, care au departamentul și nu au timp. Responsabililor cu protecția datelor și auditorilor, care trebuie să traducă obligațiile legale în măsuri pe care cineva chiar să le aplice. Și oricui a primit vreodată un apel de la „director",

„bancă” sau „copilul meu” care cerea bani urgent și s-a întrebat, după, cum ar fi putut ști.

Cartea poate fi citită de la un capăt la altul într-o după-amiază. Dar este scrisă ca să fie deschisă din nou, la fișa potrivită, în ziua în care o veți avea nevoie.

1. Parola de recunoaștere



> **Într-o frază →** un cuvânt sau o întrebare convenită dinainte, față în față, pe care doar persoana reală o poate da — o verificare pe care o voce clonată cu AI nu o poate trece, oricât de perfectă ar fi, atât timp cât secretul nu a fost compromis.

Epocă: antichitate → Al Doilea Război Mondial · Amenințare: fraudă cu deepfake / voce clonată, „CEO fraud" · Cost: zero

Originea

Cea mai veche descriere tehnică a unei parole militare o avem de la Polibiu, în *Istoriile* sale (cartea VI), unde explică cum funcționa *tessera* în legiunile romane. În fiecare seară, tribunul alegea cuvântul de ordine și îl scria pe o tăbliță de lemn. Tăblița trecea din mână în mână, de la un manipul la următorul, fiecare comandant confirmând că a primit-o, până ajungea înapoi la tribun înainte de lăsarea întunericului. Dacă tăblița nu se întorcea, se știa exact în ce manipul s-a oprit — și cineva răspundea. Două lucruri sunt remarcabile aici. Parola se schimba zilnic și exista un lanț de custodie verificabil. Romanii au inventat, practic, rotația cheilor și jurnalul de acces, cu două mii de ani înainte de orice server.

Mai veche încă este versiunea din *Cartea Judecătorilor* (12, 5–6). După o bătălie, galaadiții păzeau vadurile Iordanului și le cereau efraimiților fugari să pronunțe „șibolet". Efraimiții nu puteau rosti sunetul „ș" și spuneau „sibolet" — și erau descoperiți. Este prima parolă din istorie care nu se baza pe un secret, ci pe o trăsătură pe care impostorul nu o putea imita. Rețineți ideea; ne întoarcem la ea.

Iar cea mai cunoscută formă modernă este din noaptea de 5 spre 6 iunie 1944. Parașutiștii americani aruncați peste Normandia, împrăștiați în întuneric printre soldați germani, se identificau prin provocare și răspuns. Unul striga „Flash", celălalt

trebuia să răspundă „Thunder”, iar primul confirma cu „Welcome”. Cuvintele au fost alese și pentru că un vorbitor nativ de germană le pronunță greu — din nou, șibolet. Sistemul era de unică folosință, valabil pentru acea noapte și apoi înlocuit.

Surse: Polibiu, Istorii, VI, 34–35; Judecătorii 12, 5–6; S. L. A. Marshall, Night Drop (1962), pentru parolele din Normandia.

Principiul

Parola de recunoaștere rezolvă o problemă precisă — **cum verifici identitatea cuiva când canalul prin care comunici nu este de încredere.** Pe câmpul de luptă, canalul era întunericul și uniforma, care se poate fura. Azi, canalul este vocea, chipul de pe un apel video și numărul de telefon, toate falsificabile.

Trei proprietăți fac tehnica să funcționeze. Secretul a fost schimbat pe un alt canal decât cel atacat, adică față în față, nu prin e-mail sau WhatsApp. Este efemer, se schimbă des și, ideal, este valabil pentru o singură tranzacție. Și se bazează pe ceva ce impostorul nu poate obține din exterior, nici din înregistrări publice, nici din rețelele sociale.

În limbaj modern, este o verificare *out-of-band* cu secret partajat și rotație. Nu este autentificare cu mai mulți factori în sensul tehnic — nu înlocuiește MFA pe conturi — ci un control organizațional care acoperă exact locul unde MFA nu ajunge: decizia unui om de a executa o cerere primită de la alt om.



Amenințarea de azi

În iulie 2024, un director de la Ferrari a primit pe WhatsApp mesaje care păreau să vină de la CEO-ul Benedetto Vigna, de pe un număr nou, cu fotografia de profil a acestuia, despre o achiziție mare și confidențială. A urmat un apel telefonic. Vocea clonată imita aproape perfect accentul sud-italian al lui Vigna, iar „CEO-ul” cerea o tranzacție de acoperire valutară pentru o afacere legată de China. Directorul a sesizat mici inconsistențe în voce și cererea financiară neobișnuită, apoi a făcut exact ce făceau parașutiștii în Normandia — l-a întrebat pe apelant care era titlul cărții pe care Vigna i-o recomandase cu câteva zile înainte. Escrocul nu a putut răspunde și a închis.

Ce *nu* a mers la Ferrari este lecția. Directorul a improvizat. A avut noroc că exista o informație recentă, personală, pe care o putea folosi. Într-o firmă în care CEO-ul nu recomandă cărți, sau în care apelul ar fi ajuns la un contabil care nu vorbise niciodată cu directorul, nu exista nicio întrebare de pus. O companie din Hong Kong a pierdut aproximativ 25 de milioane de dolari exact așa, la începutul lui 2024, după ce un angajat din departamentul financiar a fost convins într-un apel video în care toți „colegii" erau deepfake-uri.

Costul unei clonări de voce este azi de ordinul minutelor și al câtorva secunde de înregistrare — un interviu, un webinar, un mesaj vocal. Pentru atacator, vocea și chipul nu mai sunt dovezi de identitate. Pentru majoritatea organizațiilor, încă sunt. În acest decalaj se face frauda. Parola de recunoaștere nu este singurul răspuns și nici cel principal pentru plăți — acolo, verificarea pe un canal independent și aprobarea separată (fișa 2) rămân baza —, dar este cel mai ieftin și singurul pe care îl poți pune în funcțiune în aceeași zi.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Adunați, fizic, în aceeași cameră, persoanele care pot aproba plăți, schimba datele bancare ale furnizorilor sau acorda acces la sisteme. De obicei sunt trei până la cinci. Conveniți un cuvânt de verificare — nu numele câinelui, nu orașul natal, nimic ce apare pe Facebook, ci un cuvânt arbitrar, ușor de reținut, fără legătură cu firma.

Regula este simplă și fără excepții. Orice cerere de plată, de schimbare a unui IBAN sau de acces „urgent și confidențial", venită prin telefon, mesaj sau video, se verifică cerând cuvântul — și, pentru plăți, se confirmă suplimentar printr-un apel inițiat de voi, la numărul din agendă, nu la cel de pe care a venit cererea. Fără cuvânt și fără confirmare, nu se execută nimic, indiferent cine pare că cere și cât de presant este tonul. Cuvântul nu se scrie în niciun sistem, nici în e-mail, nici în Teams, nici într-un fișier „parole.xlsx". Trăiește doar în memorie și se schimbă trimestrial, precum și imediat ce cineva părăsește grupul.

Firma de 500 de oameni

Un singur cuvânt nu scalează. Aici regula devine *call-back* — orice cerere financiară primită pe un canal se confirmă pe un alt canal, folosind un număr de telefon din agenda internă, nu din mesajul primit. Pentru conducere, păstrați cuvântul de recunoaștere pentru cercul restrâns, adică director general, director financiar, trezorerie și administratorii IT, exact cei care sunt ținta fraudei de tip „CEO". Combinați-l cu regula celor doi (fișa 2) pentru orice plată peste un prag, pentru că nicio voce, oricât de reală, nu poate înlocui a doua semnătură, și păstrați MFA pe toate conturile — parola verbală protejează decizia, MFA protejează contul. Scrieți regula în procedura de plăți și includeți-o în instruirea anuală, cu cazul Ferrari ca exemplu, pentru că rămâne în minte.

Acasă



Același lucru cu familia. Apelul „Mamă, am avut un accident, am nevoie de bani acum”, cu vocea copilului, este deja o fraudă curentă în România. Un cuvânt de familie, convenit la masă, rezolvă problema în trei secunde.

Unde eșuează

Secretul scris devine secret furat. Dacă cuvântul ajunge într-un e-mail, un atacator care a compromis căsuța poștală — lucru frecvent în fraudele de tip BEC — îl are înaintea voastră.

Tehnica nu rezistă la amenințarea internă. Cineva din grup poate fi atacatorul sau poate fi constrâns. De aceea se combină cu regula celor doi, nu o înlocuiește.

Apoi este presiunea psihologică. Atacatorul va spune că nu are timp de jocuri și că se pierde contractul. Romanii nu negociau parola la poartă; nici voi. Regula trebuie să fie absolută tocmai pentru că momentul atacului este construit ca să pară excepțional.

Întrebarea improvizată, varianta Ferrari, merge doar dacă există istoric comun. Convenția dinainte nu depinde de noroc. Iar istoric, parolele au picat când erau previzibile sau reutilizate — același motiv pentru care pică și azi.

Cadrul legal

Pentru entitățile NIS2, parola de recunoaștere se încadrează la art. 21 alin. (2) lit. (i) din Directiva (UE) 2022/2555 — politici de control al accesului și securitatea resurselor umane — ca procedură de autorizare a operațiunilor; ea nu ține locul autentificării cu mai mulți factori cerute la lit. (j), care rămâne o obligație distinctă pentru conturi și sisteme. Sub GDPR, art. 32 cere măsuri adecvate riscului împotriva accesului neautorizat, iar schimbarea datelor bancare ale unui salariat sau furnizor pe baza unui apel neverificat este o încălcare de securitate de care răspunde operatorul. În ISO/IEC 27001:2022, controalele A.5.17 (informații de autentificare), A.6.3 (conștientizare și instruire) și A.5.3 (separarea sarcinilor) sunt cele în care o astfel de procedură se documentează.

2. Regula celor doi



> **Într-o frază →** nicio acțiune critică nu poate fi dusă la capăt de o singură persoană — este nevoie de două chei, două semnături sau două aprobări, deținute de oameni diferiți.

Epocă: Renaștere → Războiul Rece · Amenințare: fraudă prin transfer bancar (BEC), amenințare internă, preluarea conturilor de administrator · Cost: zero până la o zi de configurare

Originea

În 1503, Coroana spaniolă a înființat la Sevilla *Casa de Contratación*, instituția care administra tot comerțul cu Lumea Nouă. Banii, aurul și documentele se păstrau într-o ladă cu trei încuietori, *arca de tres llaves*, ale cărei chei erau ținute de trei funcționari diferiți — trezorierul, factorul și contabilul. Lada nu putea fi deschisă decât în prezența tuturor trei. Nu era o măsură de încredere, ci de neîncredere organizată. Coroana presupunea că oricare dintre ei poate fi corupt și construia sistemul astfel încât corupția unuia singur să nu fie suficientă.

Același principiu apare în Anglia în 1538, când injuncțiunile lui Thomas Cromwell obligă fiecare parohie să țină un registru al botezurilor, căsătoriilor și înmormântărilor într-o ladă sigură cu două încuietori, o cheie la preot și cealaltă la epitropi. Multe dintre aceste lăzi, cu trei sau chiar patru încuietori, se mai găsesc și azi în bisericile engleze. Lada cu mai multe chei a devenit, timp de secole, forma standard de păstrare a banilor publici, a arhivelor și a actelor de proprietate în toată Europa.

Versiunea care a dat numele tehnicii este însă din Războiul Rece. După 1962, forțele nucleare americane au formalizat *two-person rule*, regula celor două persoane, potrivit căreia niciun om nu poate rămâne singur lângă o armă nucleară sau lângă sistemele ei de comandă. În centrele de lansare Minuteman, cei doi ofițeri de serviciu trebuie să rotească simultan două chei, în două console amplasate suficient de departe una de

alta încât o singură persoană să nu le poată atinge pe amândouă în același timp. Sistemul nu presupune că ofițerii sunt necinstiți. Presupune că, într-o zi, unul dintre ei ar putea fi — sau ar putea fi constrâns, păcălit ori pur și simplu greși — și face ca acea zi să nu conteze.

Surse: Archivo General de Indias, fondul Casa de la Contratación; injuncțiunile lui Thomas Cromwell (1538), art. 12; Eric Schlosser, Command and Control (2013), pentru regula celor două persoane.

Principiul

Regula celor doi separă *capacitatea* de a face o acțiune de *autoritatea* de a o face. O persoană poate iniția, dar nu poate finaliza. Efectul cel mai evident este că un atacator trebuie să compromită doi oameni, nu unul, iar dificultatea nu se dublează, ci crește exponențial, pentru că cei doi trebuie compromiși în același timp, pe același subiect, fără ca niciunul să-l alerteze pe celălalt. Al doilea efect este că eroarea umană capătă un filtru. A doua pereche de ochi prinde IBAN-ul greșit, factura dublată, comanda dată din grabă. Al treilea este că și coerciția devine vizibilă. O persoană constrânsă nu poate executa singură, iar cel de-al doilea are ocazia să observe că ceva nu este în regulă.

În criptografie, principiul are o formă matematică — partajarea secretului propusă de Adi Shamir în 1979, în care o cheie este împărțită în mai multe fragmente și un număr minim dintre ele, de exemplu două din trei, este necesar pentru reconstituire. Este lada cu trei încuietori, scrisă în algebră.



Amenințarea de azi

În ianuarie 2024, un angajat din biroul din Hong Kong al firmei de inginerie Arup a participat la un apel video cu directorul financiar și mai mulți colegi, în care i s-a cerut să execute o serie de transferuri. Toți participanții, în afară de el, erau deepfake-uri. A făcut 15 transferuri, în total aproximativ 200 de milioane de dolari Hong Kong, adică circa 25 de milioane USD, înainte ca cineva să verifice cu sediul central. Detaliul care contează nu este tehnologia deepfake, ci faptul că *un singur om putea executa 15 transferuri de această mărime fără o a doua aprobare independentă*. Vocea clonată a fost arma; absența regulii celor doi a fost vulnerabilitatea.

Același tipar se repetă în atacurile ransomware. Grupurile care compromit o rețea caută un singur cont de administrator de domeniu. Odată obținut, pot dezactiva protecția, șterge copiile de siguranță și cripta totul într-o noapte. Dacă dezactivarea soluției antivirus sau ștergerea copiilor de rezervă ar cere o a doua aprobare, atacul s-ar opri — sau măcar ar lăsa o urmă pe care cineva o vede la timp.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Stabiliți un prag, de exemplu 5.000 de lei sau orice plată către un beneficiar nou, peste care orice transfer bancar cere două aprobări în aplicația băncii. Practic toate băncile românești oferă semnături multiple pe conturile de firmă, gratuit; trebuie doar activată opțiunea. Orice schimbare a datelor bancare ale unui furnizor sau salariat se face numai cu confirmarea a doi oameni, dintre care unul sună furnizorul pe numărul vechi din agendă.

Administrarea de zi cu zi se face cu conturi individuale, nominale, cu MFA activat, nu cu un cont „administrator" partajat. Contul de urgență al domeniului — cel care rămâne când totul altceva a căzut — este altceva. Soluția corectă este un seif de secrete cu acces de urgență controlat (două persoane, consemnare, alertă), cu copii de recuperare offline și cu o procedură testată. Pentru firma care nu are încă așa ceva, varianta de avarie este cea veche de cinci sute de ani: parola nu o știe nimeni în întregime, jumătate stă într-un plic sigilat la administrator, cealaltă jumătate într-un plic la director (vezi fișa 4), iar deschiderea lor se consemnează și declanșează schimbarea parolei. Este lada cu două chei, nu o practică de administrare; regula celor doi se aplică aici accesului de urgență, nu muncii curente.

Firma de 500 de oameni

Acțiunile privilegiate din IT — crearea unui cont de administrator, dezactivarea antivirusului, modificarea politicilor de backup, schimbarea regulilor de firewall — trec printr-un sistem de gestionare a accesului privilegiat cu aprobare de la o a doua persoană. Majoritatea soluțiilor comerciale și câteva gratuite oferă fluxul. Conturile de urgență, *break-glass*, există, dar deschiderea lor declanșează o alertă către doi oameni și o revizuire a doua zi.

În procedura financiară, separarea sarcinilor devine regulă. Cine introduce o plată nu o poate și aproba; cine creează un furnizor nu poate și plăti către el. Verificați trimestrial că a doua aprobare este reală, nu un clic automat.

Unde eșuează

Coluziunea este limita evidentă. Doi oameni care se înțeleg înving sistemul. De aceea perechea trebuie să fie compusă din persoane din departamente diferite, cu interese diferite, și de aceea rotirea periodică a celui de-al doilea aprobator contează.

Cel mai frecvent mod de eșec este însă semnătura de complezență. A doua persoană aprobă fără să se uite, pentru că „Ion știe ce face”. Regula celor doi nu funcționează dacă a doua persoană nu are timp, informație și permisiunea reală de a spune nu.

Urmează ocolirea „pentru că e urgent”. Dacă procedura permite excepții când al doilea aprobator este în concediu, atacatorul va aștepta concediul. Soluția este un al treilea aprobator de rezervă, nu renunțarea la regulă. Iar fricțiunea este reală — aplicată la tot, regula paralizează. Aplicată doar la acțiunile ireversibile, adică bani, ștergeri și privilegii, costă câteva minute pe săptămână.

Cadrul legal

Art. 21 alin. (2) lit. (i) din Directiva NIS2 cere politici de control al accesului și de gestionare a activelor; regula celor doi aplicată acțiunilor privilegiate și plăților este o formă directă de control al accesului și de separare a sarcinilor. Ea nu este autentificare cu mai mulți factori și nu acoperă lit. (j): MFA pe conturi rămâne o cerință separată, pe care regula celor doi o completează, nu o înlocuiește. Sub GDPR, art. 32 alin. (1) lit. (b) cere capacitatea de a asigura integritatea sistemelor, iar art. 25 impune protecția datelor începând cu momentul conceperii, iar separarea sarcinilor este o măsură organizatorică clasică în ambele. În ISO/IEC 27001:2022, controalele A.5.3 (separarea sarcinilor) și A.8.2 (drepturi de acces privilegiat) sunt exact acest lucru.

3. Runbook-ul pe hârtie



> **Într-o frază →** procedura pentru cel mai rău caz trebuie să existe într-o formă pe care cel mai rău caz nu o poate distruge — tipărită, la îndemână, în afara sistemelor pe care le protejează.

Epocă: 1935 → prezent · Amenințare: ransomware, indisponibilitate totală a sistemelor, panică în primele ore · Cost: o zi de scris, o oră pe trimestru de actualizat

Originea

Pe 30 octombrie 1935, la baza aeriană Wright Field din Ohio, Boeing își prezenta noul bombardier, Model 299, viitorul B-17. Avionul era cel mai complex construit vreodată, cu patru motoare, flapsuri, elice cu pas variabil și tren de aterizare retractabil. La comenzi se afla maiorul Ployer Hill, pilotul-șef de încercări al armatei, unul dintre cei mai experimentați din țară. Avionul a decolat, s-a ridicat, s-a înclinat și s-a prăbușit. Hill și un alt membru al echipajului au murit. Cauza era un pas uitat — blocajul comenzilor, folosit la sol împotriva vântului, nu fusese eliberat înainte de decolare.

Concluzia unui ziar al vremii a fost că avionul era „prea mult pentru un singur om”. Concluzia piloților de încercare a fost alta. Avionul nu era prea complicat, dar memoria unui om, oricât de bun, sub presiune, nu este un loc sigur pentru o secvență de treizeci de pași. Au scris pe o foaie lista verificărilor dinaintea decolării, a decolării, a zborului și a aterizării. Cu lista, B-17 a zburat aproape două milioane de kilometri fără accident și a devenit avionul care a câștigat războiul aerian din Europa. Lista de verificare nu a fost o invenție tehnologică. A fost admiterea că, în cel mai important moment, experiența nu înlocuiește procedura.

Marina britanică avea de secole o variantă, *Night Order Book*, caietul în care căpitanul scria, înainte de a merge la culcare, ce trebuie să facă ofițerul de cart dacă se schimbă vântul, dacă apare un vas, dacă se rupe ceva. Caietul stătea pe masa de navigație, nu

într-un sertar încuiat și nu în cabina căpitanului. Stătea acolo unde era nevoie de el, la ora la care era nevoie de el.

Surse: Atul Gawande, The Checklist Manifesto (2009), cap. 2, pentru accidentul Model 299; raportul oficial al Army Air Corps din 1935; N. A. M. Rodger, The Command of the Ocean (2004), pentru practica ordinelor de noapte.

Principiul

Un plan de răspuns la incidente care se află exclusiv în sistemele informatice ale organizației are o proprietate neplăcută. Devine inaccesibil exact în momentul în care este necesar. Ransomware-ul criptează și SharePoint-ul în care este planul, și serverul de e-mail prin care s-ar trimite, și agenda cu numărul avocatului.

Runbook-ul pe hârtie exploatează două invariante. Primul este independența de eșec — suportul planului nu trebuie să aibă nicio dependență comună cu sistemele pe care planul le salvează, iar hârtia nu are driver de rețea. Al doilea este decizia luată la rece pentru momentul fierbinte. În primele ore ale unui incident, oamenii nu gândesc clar. Lista spune ce să facă în ordine, astfel încât să nu fie nevoie să gândească clar, ci doar să citească și să bifeze.



Amenințarea de azi

Pe 27 iunie 2017, atacul NotPetya a lovit grupul de transport maritim Maersk. În câteva ore, aproximativ 49.000 de laptopuri și mii de servere erau inutilizabile, în 76 de porturi din întreaga lume. Angajații au trecut la WhatsApp pe telefoanele personale, la foi Excel pe laptopuri private și la hârtie pentru a continua să descarce containere. Compania a reconstruit infrastructura în aproximativ zece zile, iar pierderile raportate au fost de 250–300 de milioane de dolari. Detaliul care a salvat Maersk — un singur controler de domeniu din Ghana care supraviețuise pentru că o pană de curent îl deconectase în momentul atacului — spune totul despre cât de subțire este linia dintre recuperare și dezastru.

În martie 2019, producătorul norvegian de aluminiu Norsk Hydro a fost lovit de ransomware-ul LockerGoga în 170 de locații. Compania a refuzat să plătească, a trecut fabricile pe operare manuală și a condus timp de săptămâni pe baza procedurilor

tipărite și a muncitorilor mai vechi care încă știau să opereze liniile fără calculator. Costul a fost de aproximativ 70 de milioane de dolari, dar producția nu s-a oprit.

Pentru o firmă românească de mărime medie, scenariul tipic este mai prozaic. Luni dimineață, nimeni nu se poate loga, pe ecrane este o notă de răscumpărare, iar planul de răspuns la incidente, dacă există, este un PDF pe serverul care tocmai a fost criptat. Primele patru ore se pierd căutând numărul firmei de IT și întrebându-se cine are voie să decidă ce.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Pregătiți „pachetul de incident", un dosar tipărit în două exemplare, unul la sediu, dar nu în camera serverelor, și unul acasă la director sau la un asociat. Conținutul lui, în ordinea în care este nevoie de el, este singura listă pe care merită să o ținem în această carte, pentru că lista este chiar tehnica.

1. **Prima pagină, primele zece acțiuni.** Deconectați de la rețea, fără să opriți, echipamentele afectate. Nu plătiți, nu negociați, nu reinstalați nimic. Fotografiați ecranele. Sunați persoanele de la punctul 2. Începeți jurnalul de la punctul 5.
2. **Lista de telefoane**, pe hârtie, cu numere personale — administratorul IT sau furnizorul de servicii IT, directorul, responsabilul cu protecția datelor, avocatul, banca pentru blocarea plăților, asiguratorul, furnizorul de internet, linia de urgență 1911 a Directoratului Național de Securitate Cibernetică.
3. **Ce trebuie evaluat, notificat și în cât timp.** Dacă sunt afectate date personale, evaluați riscul pentru persoanele vizate și documentați incidentul; dacă încălcarea este susceptibilă să genereze un risc, notificați ANSPDCP fără întârzieri nejustificate și, dacă este posibil, în cel mult 72 de ore de la luarea la cunoștință (art. 33 GDPR), iar dacă riscul este ridicat, informați și persoanele (art. 34). Dacă sunteți entitate NIS2 și incidentul este semnificativ în sensul legii, avertizare timpurie la DNSC în 24 de ore și notificare în 72 de ore. Clienții și partenerii, dacă îi afectează. Criteriile de evaluare stau scrise în dosar, ca să nu le decideți în panică.
4. **Unde sunt copiile de rezervă** și cum se restaurează fără acces la sistemele obișnuite, inclusiv parola consolei de backup, în plic sigilat (fișa 4).
5. **Jurnalul incidentului** — pagini goale, liniate, cu coloanele oră, cine, ce a făcut, ce a observat. Va fi cel mai important document la notificarea autorității și la discuția cu asiguratorul.

Păstrați și un laptop care nu a fost niciodată în domeniul firmei, cu un stick USB cu instalările de bază, pentru a avea de unde lucra.

Firma de 500 de oameni

Același pachet, dar pe roluri — o versiune pentru echipa de criză, una pentru IT, una pentru comunicare, una pentru fiecare sucursală. Exemplare tipărite stau la fiecare locație și la domiciliile a trei persoane din echipa de criză, iar o copie electronică pe un

serviciu *complet separat* de infrastructura firmei, cu alt furnizor, alt cont și alte credențiale.

De două ori pe an se face un exercițiu pe masă. Se citește scenariul, se deschide dosarul, se urmează pașii cu ceasul în mână. Veți descoperi că trei numere de telefon sunt vechi și că nimeni nu știe cine are cheia de la camera serverelor. Acesta este scopul exercițiului.

Unde eșuează

Primul eșec este versiunea veche. Un runbook tipărit în 2023 și neactualizat are numărul fostului administrator IT. Puneți o dată pe copertă și un memento trimestrial în calendar. Al doilea este dosarul pe care nu-l găsește nimeni, pentru că stă „pe undeva prin biroul contabilei” în loc să fie în același loc, cunoscut de toată echipa de criză.

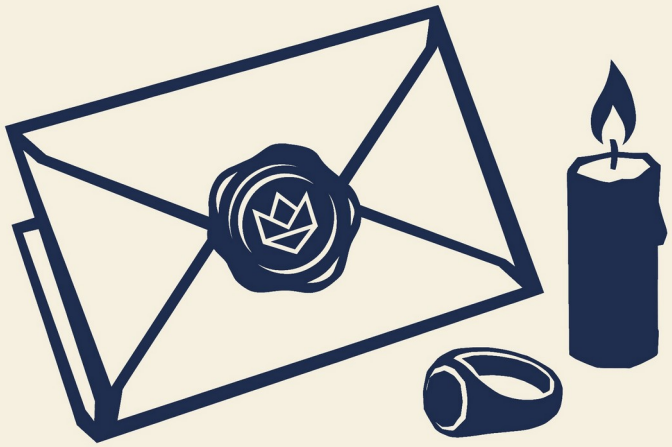
Al treilea este planul care presupune că sistemele merg. Dacă un pas spune „trimiteți e-mail la toți angajații”, planul nu a fost scris pentru ransomware. Apoi, hârtia se fură și arde, așa că dosarul conține numere de telefon și proceduri, nu parole în clar; parolele stau în plicuri sigilate separate.

Și, în sfârșit, runbook-ul nu înlocuiește pregătirea. Lista de verificare din 1935 funcționa pentru că piloții erau pregătiți și apoi aveau lista. Un runbook citit prima oară în timpul incidentului ajută, dar un runbook exersat salvează.

Cadrul legal

Art. 21 alin. (2) lit. (b) din Directiva NIS2 cere gestionarea incidentelor, iar lit. (c) continuitatea activității, gestionarea copiilor de rezervă și gestionarea crizelor; art. 23 impune, pentru incidentele semnificative, avertizarea timpurie în 24 de ore și notificarea în 72 de ore, termene greu de respectat fără un plan accesibil în afara sistemelor compromise. Sub GDPR, art. 33 cere evaluarea riscului și, când este cazul, notificarea autorității fără întârzieri nejustificate și, dacă este posibil, în 72 de ore de la luarea la cunoștință, iar art. 33 alin. (5) documentarea fiecărei încălcări, notificate sau nu; jurnalul pe hârtie este exact această documentare. În ISO/IEC 27001:2022, controalele A.5.24–A.5.28 (gestionarea incidentelor) și A.5.29–A.5.30 (continuitate și pregătirea TIC) acoperă întregul lanț.

4. Sigiliul



> **Într-o frază →** un secret păstrat într-un înveliș care nu poate fi deschis fără să lase urme — astfel încât nu împiedici accesul, dar îl faci imposibil de ascuns.

Epocă: Mesopotamia, c. 3500 î.Hr. → prezent · Amenințare: pierderea sau furtul parolelor de recuperare, al cheilor de backup și al credențialelor de urgență · Cost: câteva zeci de lei

Originea

Cu mai bine de cinci mii de ani în urmă, negustorii din Mesopotamia țineau evidența mărfurilor cu jetoane de lut, un jeton pentru o oaie, altul pentru o măsură de grâu. Când trimiteau marfa, jetoanele erau închise într-o sferă goală de lut, numită azi *bulla*, iar pe suprafața ei umedă se rula sigiliul-cilindru al expeditorului, lăsând o imagine continuă, imposibil de refăcut fără cilindrul original. Destinatarul spărgea sfera și compara jetoanele cu marfa primită. Dacă sfera ajungea spartă sau cu sigiliul alterat, știa că cineva umblase la conținut. Sigiliul nu împiedica furtul. Făcea furtul vizibil. Arheologii consideră că din aceste *bullae* s-a născut scrisul însuși, când cineva a observat că este mai simplu să imprimi jetoanele pe suprafața sferei decât să le închizi înăuntru.

Romanii purtau sigiliul pe deget, în inel, și îl aplicau în ceară pe documente și pe lădițele cu obiecte de valoare. Pliniu cel Bătrân se plângea deja, în secolul I, că inelul cu sigiliu ajunsese necesar pentru a proteja până și proviziile din cămară de propriii sclavi. În Evul Mediu, sigiliul de ceară a devenit atât semnătura, cât și plicul. O scrisoare era pliată, închisă cu ceară și marcată cu sigiliul expeditorului, astfel încât destinatarul știa două lucruri deodată, de la cine vine și dacă a mai citit-o cineva pe drum. Ruperea sigiliului unei scrisori regale era infracțiune în sine, indiferent de conținut.

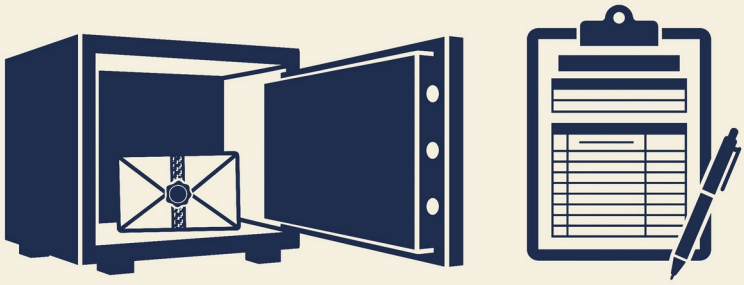
Surse: Denise Schmandt-Besserat, How Writing Came About (1996), pentru bullae; Pliniu cel Bătrân, Naturalis Historia, XXXIII, 6; Brigitte Bedos-Rezak, When Ego Was Imago (2011), pentru sigiliile medievale.

Principiul

Sigiliul rezolvă o problemă pe care criptografia nu o rezolvă — **ce faci cu secretele care trebuie să rămână accesibile.** Parola contului de administrator de urgență, cheia de recuperare a discului criptat, codurile de rezervă pentru autentificarea cu doi factori, fraza de recuperare a unui portofel, toate trebuie să existe undeva, în clar, pentru ziua în care cel care le știe nu mai este disponibil. Nu le poți memora și nu le poți pune într-un sistem care depinde tocmai de ele.

Sigiliul oferă trei lucruri deodată. O dovadă de integritate, pentru că știi dacă secretul a fost accesat. O dovadă de origine, pentru că știi cine l-a pus acolo. Și un moment de decizie, pentru că ruperea sigiliului este un act deliberat, consemnat, nu o consultare furișă.

Termenul modern este *tamper-evident* — nu rezistent la manipulare, ci evidențiind manipularea. Diferența este esențială și adesea uitată. Punga sigilată de la bancă nu este un seif. Este un martor.



Amenințarea de azi

Două scenarii se repetă în practica oricărui consultant de securitate.

Primul. Administratorul IT pleacă, se îmbolnăvește sau pur și simplu nu răspunde la telefon într-o duminică, iar parola serverului, a consolei de backup sau a contului de administrator al domeniului era doar în capul lui. Firma descoperă că nu își poate accesa propriile sisteme. Soluția improvizată, „să-i dăm și directorului parola pe WhatsApp", creează a doua problemă, pentru că acum secretul există în clar într-un mesaj, pe două telefoane, în două copii de rezervă în cloud.

Al doilea. Criptarea discurilor cu BitLocker sau FileVault este activată, corect, pe toate laptopurile. Un angajat schimbă placa de bază sau uită parola. Cheia de recuperare de 48 de cifre nu a fost salvată nicăieri, sau a fost salvată într-un fișier Excel pe un server

partajat, accesibil tuturor, unde a stat trei ani. Oricare dintre cele două variante este un eșec; a doua este o încălcare de securitate care așteaptă să fie descoperită.

Grupurile de ransomware caută explicit aceste fișiere. Un document numit „parole.xlsx” sau „recovery keys.txt” pe un server partajat este, pentru un atacator ajuns în rețea, mai valoros decât orice vulnerabilitate tehnică.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Cumpărați pungi de securitate cu sigiliu numerotat, cele folosite de bănci pentru numerar, care se găsesc la zeci de lei suta, sau, la limită, plicuri obișnuite semnate peste clapetă și acoperite cu bandă transparentă. Scrieți de mână, pe o foaie, doar secretele de urgență — cele care nu se folosesc niciodată în munca de zi cu zi: parola contului de urgență al domeniului, parola consolei de backup, cheia de recuperare a criptării, codurile de rezervă pentru MFA ale conturilor critice (bancă, domeniu, e-mail), parola routerului. Parolele de lucru curente stau într-un manager de parole, cu MFA, nu în plic. Nu tipăriți din calculator, pentru că imprimanta are memorie.

Puneți foaia în pungă și notați numărul sigiliului, data și cine a sigilat, pe un registru ținut separat; o foaie în dosarul de incident din fișa 3 este suficientă. Păstrați punga într-un seif sau într-un sertar încuiat, la care au acces două persoane (fișa 2), și o a doua pungă, identică, în alt loc, la un asociat, la avocat sau într-o casetă bancară.

Regula este că ruperea sigiliului se consemnează, se explică, și toate parolele din pungă se schimbă în săptămâna următoare și se resigilează. Verificați integritatea sigiliilor la fiecare trei luni — este o linie în registru și durează un minut.

Firma de 500 de oameni

Secretele de urgență stau într-un modul hardware de securitate sau într-un seif de parole cu funcție de *break-glass*, dar cheile de recuperare ale acestora, cele care deblochează totul, stau în plicuri sigilate, împărțite între două sau trei persoane, în locații diferite. Deschiderea unui plic declanșează automat un incident de securitate de nivel scăzut, cu notificare, justificare scrisă și rotirea secretului în 72 de ore. Auditul anual verifică fizic sigiliile și registrul, iar un sigiliu lipsă fără consemnare în registru este o neconformitate majoră.

Unde eșuează

Sigiliul se poate ridica. Ceara se înmoaie, banda se dezlipește cu căldură, o pungă poate fi tăiată și înlocuită dacă nimeni nu notează numărul. Fără registru, sigiliul este decor.

Există și copia făcută înainte de sigilare. Dacă secretul a fost tipărit, scris într-un e-mail sau fotografiat înainte să ajungă în pungă, punga păzește doar una dintre copii. Scrieți de mână și distrugeți ciornele.

Apoi vine registrul pe care nu-l verifică nimeni. Dovada există, dar nimeni nu se uită, iar verificarea trimestrială este partea care face sistemul să funcționeze. Focul și inundația fac din hârtia dintr-un singur loc un singur punct de eșec, de aceea există a doua pungă, în altă clădire. Și, în sfârșit, secretul care s-a schimbat între timp — parola din pungă este cea de acum doi ani. Orice schimbare a unui secret de urgență înseamnă o pungă nouă.

Cadrul legal

Art. 21 alin. (2) lit. (h) din Directiva NIS2 cere politici privind utilizarea criptografiei și, implicit, gestionarea cheilor; a avea cheile de recuperare într-un loc controlat este condiția ca criptarea să conteze. Sub GDPR, art. 32 alin. (1) lit. (a) recomandă criptarea, iar lit. (c) cere capacitatea de a restabili accesul la date în caz de incident, iar o cheie de recuperare pierdută transformă criptarea dintr-o măsură de securitate într-o pierdere de date. În ISO/IEC 27001:2022, controalele A.8.24 (utilizarea criptografiei, inclusiv gestionarea cheilor), A.5.17 (informații de autentificare) și A.7.10 (medii de stocare) acoperă exact această practică.

5. Copia de la mănăstire



> **Într-o frază →** un text supraviețuiește nu pentru că este bine păzit, ci pentru că există în mai multe copii, în locuri diferite, dintre care cel puțin una este departe de orice foc — regula copiilor de rezervă, scrisă de călugări cu o mie de ani înainte de ransomware.

Epocă: antichitate târzie → Evul Mediu · Amenințare: ransomware, ștergere accidentală sau răuvoitoare, compromiterea contului de cloud · Cost: un disc extern și o oră pe lună

Originea

Biblioteca din Alexandria nu a dispărut într-o singură noapte, oricât de frumoasă ar fi legenda incendiului lui Cezar. A dispărut în secole, prin neglijență, tăieri de fonduri, conflicte și, mai ales, printr-o eroare de proiectare — era *unică*. Sute de mii de suluri, într-un singur loc, în grija unei singure instituții, fără copii sistematice în altă parte. Când instituția a slăbit, textele au murit cu ea. Majoritatea literaturii grecești pe care o avem azi nu s-a păstrat la Alexandria, ci în copiile făcute în altă parte.

Lecția a fost învățată de cineva cu un simț practic remarcabil. Cassiodor, fost ministru al regelui ostrogot Teodoric, s-a retras în jurul anului 540 pe moșia sa din Calabria și a întemeiat mănăstirea Vivarium cu un scop explicit, copierea cărților. În *Institutiones*, el le explică monahilor că a copia un manuscris este o formă de rugăciune și le dă instrucțiuni despre corectură, legătorie și cum se păstrează pergamentul. Regula Sfântului Benedict, scrisă în aceeași perioadă, prevede ore zilnice de lectură și, implicit, biblioteci. Pe fundamentul ei, timp de o mie de ani, fiecare mănăstire importantă din Europa a avut un *scriptorium* în care se copiau, din nou și din nou, aceleași texte. Un manuscris de la Monte Cassino era copiat la Bobbio, apoi la Fulda, apoi la Reichenau. Nu exista o politică centrală de arhivare. Exista redundanța.

Rezultatul se vede în statistici. Aproape tot ce avem din Cicero, Virgiliu, Tacit sau Seneca ne-a ajuns prin copii medievale, iar pentru multe texte copia cea mai veche care a supraviețuit vine dintr-o mănăstire aflată la mare distanță de locul unde a fost scris originalul. Când Monte Cassino a fost distrus de bombardamentele aliate în februarie 1944, manuscrisele erau deja evacuate la Roma, nu pentru că cineva avea un plan de continuitate, ci pentru că, după o mie patru sute de ani de incendii, cutremure și jafuri, „ține copia în altă parte" era reflex.

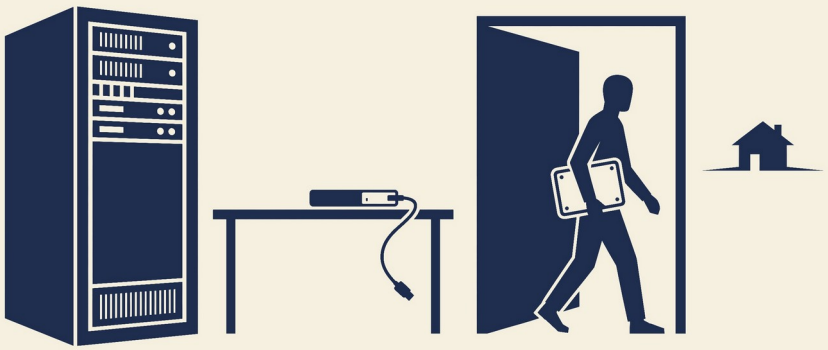
Înaintea tuturor, o lecție involuntară. Biblioteca regelui asirian Assurbanipal, de la Ninive, s-a păstrat *pentru că* palatul a ars. Focul care a distrus orașul în 612 î.Hr. a copt tăblițele de lut și le-a făcut practic indestructibile. Suportul contează.

Surse: Cassiodor, Institutiones, I, 30; L. D. Reynolds, N. G. Wilson, Scribes and Scholars (ed. a 4-a, 2013), pentru transmiterea textelor clasice; Peter Krogh, The DAM Book (2005), pentru regula 3-2-1.

Principiul

Copia de la mănăstire codifică o regulă pe care fotograful Peter Krogh a formulat-o în 2005 ca „3-2-1" și pe care orice administrator IT o știe pe de rost și o aplică rar — **trei copii, pe două tipuri de suport, una în afara locației.** Trei copii, pentru că o copie se poate corupe sau pierde fără să observi. Două suporturi, pentru că o defecțiune lovește de obicei un singur tip de dispozitiv sau un singur furnizor. Una în altă parte, pentru că focul, inundația, furtul și atacatorul lovesc un loc odată.

Ransomware-ul a adăugat un al patrulea element, pe care călugării îl aveau implicit. Copia trebuie să fie deconectată. Un manuscris de la Fulda nu putea fi ars de focul de la Monte Cassino pentru că nu exista niciun drum pe care focul să ajungă acolo. O copie de rezervă accesibilă din rețea este, pentru atacator, un fișier ca oricare altul.



Amenințarea de azi

Grupurile de ransomware moderne nu criptează imediat. Petrec zile sau săptămâni în rețea, cu un singur scop înaintea criptării, găsirea și distrugerea copiilor de rezervă. Caută serverele Veeam, consolele de backup, conturile de cloud sincronizate,

snapshot-urile de pe sistemele de virtualizare, și le șterg. Abia apoi criptează. Scopul este simplu — o victimă fără copii de rezervă plătește.

Cazul Maersk din 2017 (fișa 3) este exemplul perfect. Infrastructura mondială a companiei a fost reconstruită plecând de la un singur controler de domeniu, din Ghana, care supraviețuise doar pentru că o pană de curent îl ținuse deconectat în timpul atacului. Copia de la mănăstire a fost, în acest caz, un accident. Nu ar trebui să fie.

Al doilea scenariu, mai frecvent la firmele mici, sună așa — „avem backup, e în cloud". Dosarele sunt sincronizate cu OneDrive sau Google Drive. Când ransomware-ul criptează fișierele de pe laptop, sincronizarea încarcă fidel versiunile criptate în cloud. Sincronizarea nu este copie de rezervă; este oglindă. Oglinda reflectă și dezastrul.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Cumpărați două discuri externe. Unul stă în firmă, celălalt acasă la director sau la un asociat, și se schimbă între ele săptămânal. Discul care nu este în uz stă *deconectat*. Acesta este singurul lucru care contează cu adevărat. Configurați o copie de rezervă automată, cu orice program de backup, inclusiv cele incluse în sistemul de operare, către discul conectat, zilnic, cu criptarea copiei activată și parola pusă în plicul sigilat (fișa 4).

Păstrați sincronizarea în cloud, dar activați istoricul versiunilor și verificați că puteți restaura un fișier de acum 30 de zile. Pentru datele critice, adăugați un serviciu de backup separat de cel de stocare, cu alt furnizor și alt cont.

O dată pe lună, alegeți un fișier la întâmplare și restaurați-l de pe discul deconectat, pe alt calculator. Dacă durează mai mult de zece minute sau nu reușiți, nu aveți copie de rezervă. Aveți o speranță.

Firma de 500 de oameni

Copiile de rezervă sunt imutabile, adică nu pot fi șterse sau modificate o perioadă fixă, nici de administrator, și stau pe un sistem cu credențiale *complet separate* de domeniul principal, pentru ca atacatorul care deține domeniul să nu poată atinge consola de backup. Pentru sistemele critice, copii pe bandă sau pe un depozit offline, rotite în afara locației — banda este lentă, ieftină și, deconectată, imună.

De două ori pe an se face un test de restaurare completă a unui sistem critic, de la zero, cu timp măsurat, iar rezultatul, adică orele până la repunerea în funcțiune, intră în planul de continuitate. Orice modificare a politicii de retenție sau ștergere a snapshot-urilor se monitorizează activ, pentru că acesta este semnalul că un atac este în pregătire.

Unde eșuează

Cel mai frecvent eșec este copia netestată. Backup-ul rulează de trei ani, raportează „succes” și restaurează fișiere corupte. Testul lunar este tehnica, nu backup-ul.

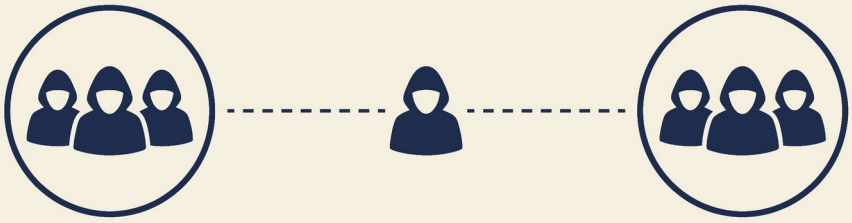
Urmează copia conectată. Un disc extern care stă permanent în USB este criptat odată cu restul, iar un NAS în rețea, cu parola de administrator implicită, este prima țintă. Apoi cheia în același loc — o copie criptată a cărei parolă este pe serverul criptat este inutilă; cheia stă în plic, în altă clădire.

Retenția prea scurtă este o capcană mai subtilă. Dacă păstrați copii de șapte zile și atacatorul a stat în rețea două săptămâni, toate copiile conțin deja malware. Păstrați copii lunare timp de un an. Și, în sfârșit, nici călugării nu copiau tot, iar ce nu părea important s-a pierdut. Decideți explicit ce intră în copia de rezervă și verificați că serverul de contabilitate instalat anul trecut chiar este inclus.

Cadrul legal

Art. 32 alin. (1) lit. (c) GDPR cere capacitatea de a restabili disponibilitatea și accesul la datele personale în timp util în caz de incident, adică, literal, obligația de a avea copii de rezervă funcționale, iar lit. (d) cere testarea periodică a măsurilor. Art. 21 alin. (2) lit. (c) din Directiva NIS2 numește explicit gestionarea copiilor de rezervă și recuperarea în caz de dezastru. În ISO/IEC 27001:2022, controlul A.8.13 (copii de rezervă ale informațiilor) cere copii testate periodic, iar A.5.30 (pregătirea TIC pentru continuitatea activității) cere obiective de timp de recuperare definite și verificate.

6. Compartimentarea



> **Într-o frază →** fiecare om știe doar ce îi trebuie ca să-și facă treaba, astfel încât compromiterea unuia singur să nu compromită întregul — regula *need-to-know*, pe care rețelele de rezistență au plătit-o cu vieți ca să o învețe.

Epocă: Al Doilea Război Mondial · Amenințare: mișcare laterală în atacurile ransomware, amenințare internă, scurgeri de date · Cost: o zi de inventariat accesele, apoi disciplină

Originea

În Franța ocupată, între 1940 și 1944, rețelele de rezistență au învățat compartimentarea pe calea cea mai dureroasă. Primele rețele erau construite natural, ca orice grup de prieteni. Toată lumea îi cunoștea pe toți, ședințele se țineau în aceleași apartamente, listele de membri existau. Când Gestapo-ul aresta un singur om și îl interoga, cădea rețeaua întreagă. Rețeaua *Interallié*, una dintre cele mai mari din 1941, a fost desființată în câteva săptămâni după arestarea unei singure persoane care știa prea mult.

Lecția a fost codificată de serviciul britanic SOE și de organizațiile franceze în structura „celulei". Grupuri de trei până la cinci oameni, în care fiecare membru cunoaște doar numele de cod al celorlalți din celulă și o singură persoană de legătură din afara ei. Agentul nu știa unde locuiesc ceilalți, nu știa ce fac celelalte celule, nu știa cine este șeful rețelei. Întâlnirile se fixau prin intermediari, mesajele prin cutii poștale moarte (fișa 8). Un om arestat putea trăda, sub tortură, cel mult patru sau cinci persoane, și nimic din ceea ce nu știa. Rețeaua supraviețuia pierderii oricărei celule.

În același timp, de cealaltă parte a oceanului, generalul Leslie Groves conducea Proiectul Manhattan cu același principiu, aplicat la o scară fără precedent. Zeci de mii de muncitori de la Oak Ridge și Hanford operau instalații uriașe fără să știe ce

produc. Fizicienii de la Los Alamos lucrau pe fragmente ale problemei. Groves a scris mai târziu că împărțirea cunoașterii pe compartimente era însăși inima securității proiectului, fiecare om știind doar ceea ce îi era strict necesar pentru sarcina lui. Proiectul a rămas, în linii mari, necunoscut publicului și Congresului până la Hiroshima.

Și totuși, Klaus Fuchs, fizician cu acces la nucleul proiectului, a transmis Uniunii Sovietice detalii esențiale. Compartimentarea nu a împiedicat scurgerea. A limitat-o la ceea ce știa Fuchs și a făcut ca zeci de mii de alți oameni să nu poată scurge nimic. Aceasta este promisiunea reală a tehnicii, nu prevenirea, ci limitarea pagubei.

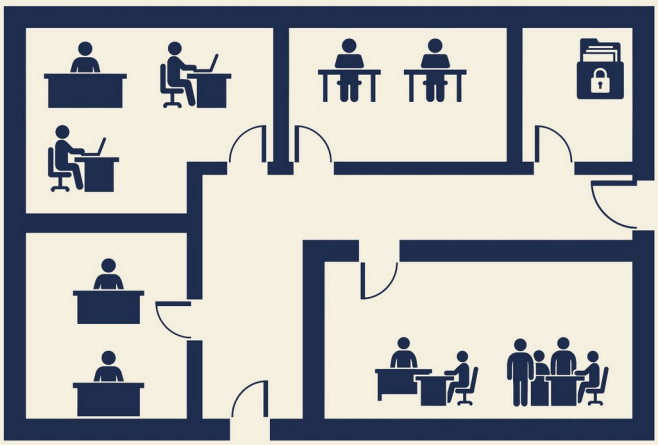
Surse: M. R. D. Foot, SOE in France (1966), cap. 4; Leslie R. Groves, Now It Can Be Told (1962), cap. 11; Richard Rhodes, The Making of the Atomic Bomb (1986), pentru cazul Fuchs.

Principiul

Compartimentarea pleacă de la o presupunere incomodă. Cineva din interior va fi compromis — nu neapărat trădător, poate păcălit de un e-mail, poate cu parola furată, poate cu laptopul lăsat în tren. Întrebarea nu este dacă, ci cât de mult poate fi pierdut atunci când se întâmplă.

Răspunsul este să proiectezi accesul astfel încât fiecare cont să vadă doar ce îi trebuie, ceea ce se numește principiul privilegiului minim. Contabila nu are acces la dosarele de personal, dezvoltatorul nu are acces la contabilitate, directorul nu are cont de administrator pe server. Apoi, compromiterea unui compartiment nu trebuie să deschidă următorul, iar rețeaua, serverele și datele sunt separate astfel încât un atacator care a intrat în laptopul unui agent de vânzări să nu poată ajunge, de acolo, la serverul de contabilitate. Și cunoașterea privilegiată este distribuită, pentru ca nimeni să nu știe tot, nici administratorul IT.

Compartimentarea și privilegiul minim sunt fundamentele pe care se construiește azi arhitectura numită *zero trust* — aceea în care nicio cerere, nici din interior, nu este considerată de încredere până nu este verificată. Zero trust adaugă peste ele verificarea continuă a identității și a dispozitivului; compartimentarea singură nu este zero trust, dar fără ea zero trust nu există. Rețeaua de rezistență din 1943 pusese temelia fără să aibă nevoie de cuvânt.



Amenințarea de azi

Aproape fiecare atac ransomware urmează același drum. Un angajat deschide un atașament sau introduce parola pe o pagină falsă, atacatorul obține controlul unui calculator obișnuit și de acolo „se mișcă lateral", căutând alte calculatoare la care contul respectiv are acces, parole salvate, partajări de rețea deschise tuturor, și urcă treptat spre contul de administrator de domeniu. Într-o rețea plată, fără compartimente, drumul de la primul laptop la controlul total durează de obicei câteva ore. Într-o rețea compartimentată, atacatorul se oprește în primul compartiment, sau face suficient zgomot încercând să iasă încât este observat.

Al doilea scenariu este cel al accesului prea larg la date. În majoritatea firmelor românești de 20–100 de angajați, serverul de fișiere are un singur dosar partajat, la care au acces toți, cu dosarele de personal, contractele, listele de clienți și ofertele într-un loc. Un singur cont compromis, al oricui, înseamnă scurgerea întregului set de date personale al firmei și o notificare la ANSPDCP care trebuie să descrie *toate* categoriile de date afectate, pentru că toate erau accesibile.

Cazul Edward Snowden, din 2013, este exemplul extrem al aceleiași probleme. Un administrator de sistem contractual, cu drepturi largi de acces pentru motive tehnice, a putut copia un volum uriaș de documente care nu aveau nicio legătură cu sarcinile lui. Compartimentarea nu lipsea din politica NSA. Lipsea din implementare.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Luați o foaie și faceți tabelul. Pe linii, fiecare angajat; pe coloane, fiecare sistem sau dosar important — contabilitate, personal, clienți, server, e-mail de administrare, bancă. Bifați cine are acces *acum*. Apoi, cu un alt pix, cine *are nevoie*. Diferența dintre cele două este lista de lucru pentru săptămâna aceasta.

Pe serverul de fișiere, înlocuiți dosarul unic cu trei sau patru dosare pe departamente, cu drepturi separate; dosarul de personal îl vede doar cine face salariile și directorul.

Nimeni nu lucrează zi de zi cu un cont de administrator, nici administratorul IT, iar contul de administrator se folosește doar pentru administrare, separat de contul cu care se citește e-mailul. Puneți rețeaua de oaspeți, cu Wi-Fi-ul pentru vizitatori, telefoanele personale, imprimanta și camerele de supraveghere, pe un segment separat de calculatoarele de lucru. Orice router de business o face din două clicuri.

Firma de 500 de oameni

Rețeaua se segmentează pe zone — utilizatori, servere, administrare, producție, oaspeți — cu reguli explicite între ele și cu principiul că, implicit, nimic nu trece dintr-o zonă în alta. Controlul accesului se face pe roluri, cu revizuire trimestrială în care fiecare manager confirmă, pe lista lui, cine mai are nevoie de ce, iar conturile celor plecați se dezactivează în ziua plecării, nu „la următoarea curățenie".

Administrarea se face de pe stații dedicate, izolate, de pe care nu se citește e-mail și nu se navighează pe internet. Datele personale sensibile, adică sănătate, salarii și evaluări, stau în sisteme separate, cu jurnalizarea fiecărui acces (fișa 12).

Unde eșuează

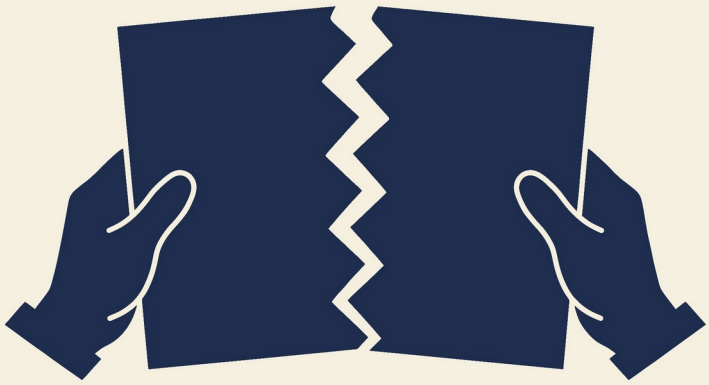
Fricțiunea naște ocoliri. Dacă oamenii nu pot ajunge la ce le trebuie, trimit fișierele pe e-mailul personal sau le pun pe un stick, iar compartimentarea prea strânsă creează un sistem paralel, necontrolat, mai periculos decât lipsa ei. Apoi este excepția permanentă — „dă-i acces lui Mihai până terminăm proiectul" devine acces pe viață, așa că orice drept temporar are o dată de expirare scrisă.

Rămâne administratorul care știe tot. Cineva trebuie să poată configura sistemul, iar acel cineva devine singurul punct de eșec. Soluția este regula celor doi (fișa 2) și jurnalizarea, nu iluzia că administratorul nu există. Rămâne și Fuchs — un om cu acces legitim la nucleu poate scurge nucleul. Compartimentarea limitează raza exploziei; nu o anulează. Iar rețelele de rezistență au eșuat și când compartimentarea era perfectă pe hârtie, dar oamenii, din prietenie, se întâlneau oricum. Procedura este cât de bună este disciplina.

Cadrul legal

Art. 5 alin. (1) lit. (c) GDPR (reducerea la minimum a datelor) și art. 25 (protecția datelor începând cu momentul conceperii și în mod implicit) cer, în esență, ca datele să fie accesibile doar celor care au nevoie de ele; art. 32 cere măsuri împotriva accesului neautorizat, iar un dosar partajat cu toată firma este un acces neautorizat în așteptare. Art. 21 alin. (2) lit. (i) din Directiva NIS2 cere politici de control al accesului și de gestionare a activelor. În ISO/IEC 27001:2022, controalele A.5.15 (controlul accesului), A.5.18 (drepturi de acces), A.8.3 (restricționarea accesului la informații) și A.8.22 (separarea rețelelor) sunt compartimentarea, pe articole.

7. Chirograful



> **Într-o frază →** un document este autentic dacă se potrivește exact cu o copie-martor păstrată în altă parte — principiul din spatele hash-ului, al semnăturii electronice și al verificării unei facturi, inventat de notari medievali cu un cuțit.

Epocă: Evul Mediu timpuriu → secolul XIX · Amenințare: facturi falsificate, actualizări de software compromise, modificarea neobservată a documentelor și jurnalelor · Cost: zero până la o aplicație de semnătură electronică

Originea

Din secolul al IX-lea și până la sfârșitul Evului Mediu, când două părți încheiau un contract — o vânzare de pământ, o arendă, o înțelegere între o mănăstire și un vecin —, scribul scria textul de două ori, sau de trei ori, pe aceeași foaie de pergament. Între copii scria, cu litere mari, cuvântul CHIROGRAPHUM, uneori CYROGRAPHUM, din grecescul „scris de mână”. Apoi tăia pergamentul prin mijlocul cuvântului, de obicei cu o linie ondulată sau zimțată, și dădea fiecărei părți câte o bucată. Dacă mai târziu una dintre părți pretindea că textul a fost altul, cele două bucăți erau puse una lângă alta. Tăietura trebuia să se potrivească perfect, iar jumătățile literelor să se îmbine. Un fals nu putea reproduce nici linia tăieturii, nici forma literelor tăiate. De la tăietura zimțată vine cuvântul englezesc *indenture*, care a însemnat „contract” timp de secole.

Chirograful rezolvă două lucruri deodată. Fiecare parte are propria copie completă și nu depinde de arhiva celeilalte, iar fiecare copie poartă dovada fizică a legăturii cu cealaltă. Nici copia, nici dovada nu puteau fi falsificate separat.

Trezoreria engleză a folosit, din jurul anului 1100 până în 1826, o variantă pentru bani, *tally stick*-ul. O bucată de lemn de alun pe care se crestau suma datorată, cu crestături de lățimi diferite pentru lire, șilingi și pence, și numele debitorului. Bățul era apoi

despicat pe lungime, prin crestături. Jumătatea mai lungă, *stock*, rămânea la creditor, cea scurtă, *foil*, la debitor. La plată, cele două jumătăți se potriveau crestătură cu crestătură. Nimeni nu putea adăuga o crestătură pe o jumătate fără ca lipsa ei de pe cealaltă să fie evidentă. Sistemul a funcționat șapte secole. A fost abolit în 1826, iar în 1834 funcționarii au hotărât să ardă tonele de bețe vechi în cuptoarele Camerei Lorzilor. Focul a scăpat de sub control și a distrus Palatul Westminster. Chiar și dispariția tehnicii a fost o lecție despre cum nu se distruge un registru.

Surse: M. T. Clanchy, From Memory to Written Record (ed. a 3-a, 2013), pentru chirografe; The National Archives (UK), colecția de tally sticks ale Trezoreriei și relatarea incendiului din 1834; Caroline Shenton, The Day Parliament Burned Down (2012).

Principiul

Chirograful separă **documentul** de **dovada integrității lui** și le păstrează în locuri diferite, sub controlul unor părți diferite. Modificarea documentului fără modificarea dovezii devine detectabilă, iar modificarea amândurora cere acces la ambele părți.

Echivalentul modern este funcția hash, o „amprentă” scurtă, de exemplu 64 de caractere pentru SHA-256, calculată din conținutul unui fișier, astfel încât orice schimbare a unui singur bit produce o amprentă complet diferită. Dacă amprenta este publicată sau păstrată pe un canal separat de fișier, destinatarul poate verifica, exact ca notarul medieval, că jumătățile se potrivesc. Semnătura electronică adaugă al doilea element al chirografului, legătura cu identitatea celui care a semnat, și îl face verificabil fără să fie nevoie ca părțile să se întâlnească.

Important este ce nu face chirograful. Dovedește că *acest* text este cel convenit. Nu dovedește că textul convenit este cinstit. Integritatea nu este autenticitate și nu este bună-credință.



Amenințarea de azi

Cea mai frecventă fraudă împotriva firmelor românești nu este un atac tehnic sofisticat. Este o factură. Atacatorul, care a compromis căsuța de e-mail a unui furnizor sau doar a observat o conversație, trimite factura reală, cu PDF-ul modificat într-un singur loc, contul bancar. Contabilitatea plătește furnizorul cunoscut, pentru

serviciul real, la suma corectă — în contul greșit. Documentul este perfect, cu antet, cu număr, cu semnătură scanată. Doar că nu se potrivește cu jumătatea pe care ar trebui s-o aibă destinatarul, IBAN-ul din contractul semnat sau de la plata precedentă.

La celălalt capăt al scalei, în decembrie 2020, s-a descoperit că atacatori de stat compromiseseră procesul de construire a software-ului SolarWinds Orion și inseraseră cod malițios într-o actualizare distribuită la aproximativ 18.000 de clienți, inclusiv agenții federale americane. Actualizarea era semnată digital, corect, de SolarWinds — chirograful se potrivea. Problema era că atacatorul modificase textul *înainte* ca scribul să-l copieze. Cazul arată limita tehnicii și de ce verificarea integrității trebuie să înceapă de la sursă (fișa 8, despre izolarea mediilor de construire), nu doar la destinatar.

Între cele două stau jurnalele de sistem modificate de atacator ca să-și șteargă urmele, contractele în Word trimise pe e-mail și „ajustate” de cealaltă parte, rapoartele de audit alterate după semnare.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Pentru facturi, orice IBAN nou sau schimbat se verifică pe un canal separat, prin telefon la numărul din contract, nu din e-mail, înainte de prima plată — jumătatea cealaltă a chirografului. Contabilitatea ține o listă tipărită a IBAN-urilor furnizorilor recurenți, actualizată doar după verificare.

Pentru documentele importante sunt două măsuri diferite, care nu se înlocuiesc una pe alta. Prima este semnătura: contractele se semnează cu semnătură electronică calificată, cu certificate de la un prestator de servicii de încredere calificat, la câteva zeci de euro pe an; ea leagă documentul de semnatar și are efectul semnăturii olografe. A doua este verificarea integrității unui fișier transmis: PDF-ul pleacă pe e-mail, iar amprenta lui SHA-256 pleacă separat, prin SMS sau WhatsApp, astfel încât destinatarul să poată verifica, înainte de a-l folosi, că a primit exact fișierul trimis. Amprenta nu spune cine l-a trimis și nu ține loc de semnătură; spune doar că fișierul nu a fost modificat pe drum. Pe Windows, comanda `certutil -hashfile fisier.pdf SHA256` o calculează fără niciun program suplimentar; pe Mac și Linux, `shasum -a 256 fisier.pdf`.

Pentru software, instalările de programe se descarcă doar de la producător, iar pentru orice instrument de administrare se verifică amprenta publicată pe site-ul oficial înainte de instalare.

Firma de 500 de oameni

Semnătura electronică se integrează în fluxul de contracte și aprobări, cu verificarea automată a validității certificatelor. Jurnalele de securitate se trimit în timp real către un sistem separat (fișa 12), cu înlănțuire criptografică, în care fiecare înregistrare conține amprenta celei precedente, astfel încât ștergerea sau modificarea unei intrări rupe lanțul vizibil.

Pentru software-ul dezvoltat intern sau achiziționat se verifică semnăturile furnizorilor, se ține un inventar al componentelor (SBOM) și se verifică amprentele la fiecare instalare, exact punctul în care SolarWinds a eșuat la clienții săi. Controlul modificărilor înseamnă că nicio schimbare nu ajunge în producție fără o înregistrare separată a ce s-a schimbat, de către cine și cu ce aprobare.

Unde eșuează

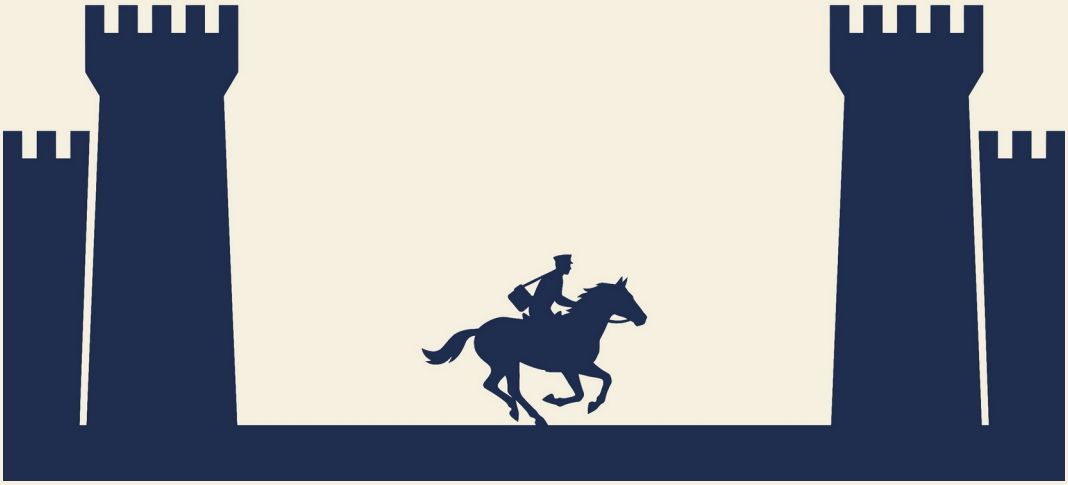
Dacă amprenta circulă pe același canal cu fișierul, atacatorul care modifică fișierul modifică și hash-ul. Jumătățile chirografului trebuie să stea în mâini diferite. Integritatea nu este autenticitate — un fișier malițios are un hash perfect valid, iar amprenta spune doar „acesta este fișierul pe care l-a publicat sursa", nu că sursa este de încredere. Când sursa este compromisă, ca la SolarWinds, ambele jumătăți sunt false și se potrivesc perfect.

Semnătura scanată nu este chirograf. O imagine a unei semnături lipită într-un PDF este, juridic, cel mult o semnătură electronică simplă: nu i se poate refuza orice efect juridic doar pentru că este electronică (art. 25 din Regulamentul eIDAS), dar nu oferă nimic din garanțiile semnăturii calificate — nu leagă documentul de semnatar și nu detectează modificările ulterioare. Chirograful cere tocmai legătura fizică sau criptografică dintre document și dovadă; imaginea nu o are. Iar dovezile de integritate trebuie păstrate cât timp contează documentul și distruse cu grijă după aceea — Westminster a ars din cauza unui registru aruncat în cuptor.

Cadrul legal

Art. 32 alin. (1) lit. (b) GDPR cere capacitatea de a asigura integritatea sistemelor și serviciilor de prelucrare, iar art. 5 alin. (1) lit. (f) o numește printre principiile prelucrării. Art. 21 alin. (2) lit. (d) și (e) din Directiva NIS2 cer securitatea lanțului de aprovizionare și a achiziției, dezvoltării și întreținerii sistemelor, iar verificarea integrității actualizărilor este măsura minimă. Regulamentul eIDAS (UE) nr. 910/2014 stabilește că semnătura electronică calificată are efectul juridic al semnăturii olografe în toată Uniunea. În ISO/IEC 27001:2022, controalele A.8.24 (criptografie), A.5.19–A.5.21 (securitatea relațiilor cu furnizorii), A.8.32 (gestionarea schimbărilor) și A.8.15 (jurnalizare) se sprijină toate pe această tehnică.

8. Mesagerul și spațiul gol



> **Într-o frază →** cel mai sigur canal este cel care nu există — informația critică se mută fizic, de un om, între sisteme care nu sunt conectate la nimic.

Epocă: Imperiul Persan → Războiul Rece · Amenințare: ransomware, acces de la distanță la sisteme critice, compromiterea mediilor de construire și a cheilor · Cost: zero până la un calculator dedicat

Originea

Herodot descrie, în cartea a VIII-a a *Istoriilor* (cap. 98), sistemul de curieri al Imperiului Persan, iar în cartea a V-a (cap. 52–54) Drumul Regal dintre Sardes și Susa pe care acesta funcționa. Stații la o zi de călărie una de alta, cu cai și călăreți odihniți, astfel încât mesajul trecea din mână în mână fără oprire — „nici zăpada, nici ploaia, nici arșița, nici întunericul nopții" nu-i opreau, scrie el într-o frază care a ajuns, peste două mii de ani, deviza poștei din New York. Ce nu spune Herodot, pentru că era evident, este de ce regele avea nevoie de un asemenea sistem. Un mesaj purtat de un om de încredere, pe un drum păzit, era singura formă de comunicare pe care un adversar nu o putea asculta de la distanță. Nu exista „de la distanță". Ca să afli ce scrie, trebuia să pui mâna pe curier.

Principiul a supraviețuit intact până azi în dreptul internațional. Convenția de la Viena din 1961 privind relațiile diplomatice stabilește, la art. 27, că valiza diplomatică nu poate fi deschisă sau reținută, iar curierul diplomatic se bucură de inviolabilitate. Statele au telefoane criptate, sateliți și rețele dedicate, și totuși continuă să trimită documentele cele mai sensibile într-o geantă, cu un om. Pentru că geanta, spre deosebire de orice rețea, are o proprietate pe care criptografia nu o poate oferi — *nu poate fi atacată de cineva care nu se află lângă ea*.

Războiul Rece a adăugat a doua tehnică, cutia poștală moartă, *dead drop*. Agentul și ofițerul de legătură nu se întâlnesc niciodată. Unul lasă mesajul într-un loc convenit, o crăpătură în zid, o piatră goală pe dinăuntru într-un parc, iar celălalt îl ridică mai târziu. Nicio transmisie, nicio întâlnire de observat, niciun moment în care ambii să fie în același loc. Comunicarea există, dar canalul nu are nicio secundă de existență simultană.

Iar în 2010 lumea a aflat cum arată eșecul acestei tehnici. Centrifugele de la Natanz, din Iran, erau controlate de o rețea izolată fizic de internet, un *air gap*, un spațiu gol. Viermele Stuxnet a ajuns totuși în ea, aproape sigur pe un stick USB, și a distrus aproximativ o mie de centrifuge. Spațiul gol fusese traversat de un om cu un stick. Mesagerul este și cea mai mare forță a tehnicii, și principala ei slăbiciune.

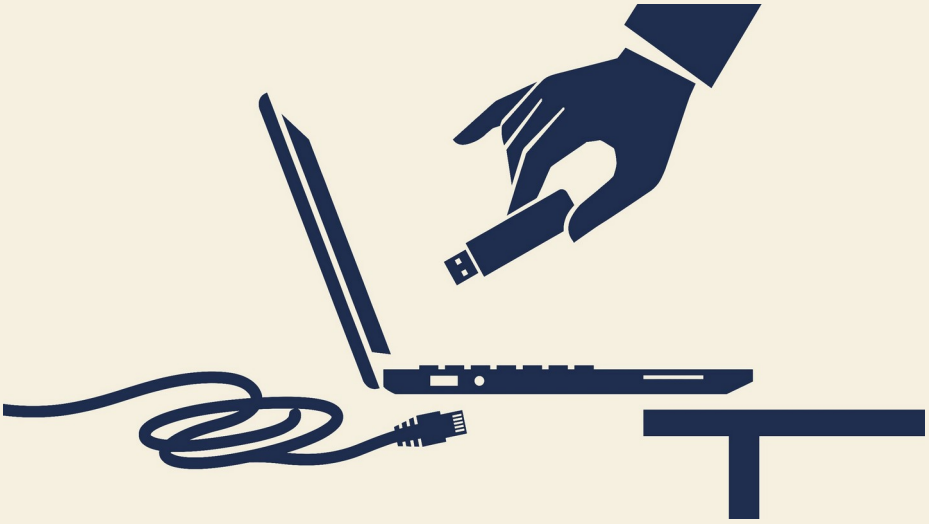
Surse: Herodot, Istorii, V, 52–54 și VIII, 98; Convenția de la Viena privind relațiile diplomatice (1961), art. 27; Kim Zetter, Countdown to Zero Day (2014), pentru Stuxnet.

Principiul

Orice sistem conectat la o rețea poate fi atacat de oriunde din acea rețea. Dacă rețeaua este internetul, „oriunde” înseamnă planeta. Spațiul gol reduce suprafața de atac la ceea ce poate ajunge fizic lângă sistem.

De aici decurg trei aplicații. Prima este izolarea a ceea ce nu are nevoie de rețea — un server de backup, o autoritate de certificare rădăcină, un sistem de control industrial, un calculator pentru semnarea software-ului, niciunul nu trebuie să poată fi atins de pe un laptop de birou. A doua este transferul controlat. Când informația trebuie să treacă spațiul gol, trece pe un suport fizic, printr-un om, cu o procedură care spune ce se transferă, cine, când și de pe ce suport verificat. A treia este întârzierea ca protecție. Cutia poștală moartă introduce timp între trimitere și primire, iar timpul este spațiul în care se poate observa că ceva nu este în regulă.

Termenul informal este *sneakernet*, rețeaua pe tenisi, în care datele circulă pe stick, purtat de cineva care merge pe jos. Este o glumă în IT. Este, și astăzi, modul în care se mută cheile cele mai importante din lume.



Amenințarea de azi

Accesul de la distanță este vectorul principal al atacurilor ransomware asupra firmelor mici și mijlocii — un port RDP deschis către internet, un VPN cu parolă slabă, un instrument de administrare de la distanță instalat „ca să putem interveni rapid”. Fiecare este o fereastră prin care atacatorul intră fără să se ridice de pe scaun. În multe cazuri, sistemul expus nu avea nevoie să fie accesibil de la distanță. Era doar comod.

Pentru infrastructura industrială și medicală, miza este alta. Un sistem de control al unei linii de producție, un echipament de imagistică medicală sau un sistem de ventilație al unei clădiri a fost proiectat pentru a funcționa izolat; conectarea lui la rețeaua de birou, pentru raportare sau mentenanță, îi dă unui atacator de ransomware acces la procese fizice. Cazul Norsk Hydro (fișa 3) a fost supraviețuit tocmai pentru că fabricile puteau fi operate manual, deconectate.

Iar pentru cheile cele mai importante, certificatul rădăcină al unei organizații, cheia de semnare a software-ului, cheia de criptare a copiilor de rezervă, un sistem conectat este un risc permanent. Cazul SolarWinds (fișa 7) a început cu accesul atacatorului la un server de construire a software-ului care era, firește, în rețea.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Închideți orice acces de la distanță care nu este strict necesar. Dacă furnizorul de IT are nevoie să intervină, accesul se deschide la cerere, pentru intervenție, și se închide după, fără să rămână permanent deschis. Copia de rezervă deconectată (fișa 5) este spațiul gol în forma cea mai ieftină, pentru că discul care nu este în priză nu poate fi criptat.

Pentru operațiunile bancare și semnăturile electronice, folosiți un laptop dedicat, pe care nu se citește e-mail, nu se navighează și nu se instalează nimic. Costă cât un laptop simplu și elimină aproape complet riscul ca o pagină falsă sau un atașament să

ajungă pe calculatorul de pe care se fac plățile. Orice stick USB care intră în firmă de la un terț se deschide întâi pe un calculator izolat, fie și un laptop vechi fără rețea, nu pe stația contabilei. Mesagerul este verificat la poartă.

Firma de 500 de oameni

Sistemele industriale, medicale și de clădire stau pe rețele separate fizic sau prin diode de date, dispozitive care permit traficul într-un singur sens, spre exterior pentru raportare și niciodată spre interior. Autoritatea de certificare rădăcină și cheile de semnare a software-ului stau pe un sistem complet deconectat, într-o cameră încuiată, pornit doar pentru operațiuni programate, cu regula celor doi (fișa 2) și jurnal (fișa 12).

Transferul de fișiere spre și dinspre zonele izolate se face printr-o stație de verificare dedicată, cu suporturi de unică folosință, cu scanare antimalware și cu consemnarea fiecărui transfer. Mediul în care se construiește software-ul livrat clienților este izolat de rețeaua de birou, cu acces restrâns și verificat — lecția directă a cazului SolarWinds.

Unde eșuează

Stick-ul, adică Stuxnet. Spațiul gol este traversat de fiecare dată de un om cu un suport, iar dacă suportul nu este verificat și transferul nu este consemnat, izolarea este o iluzie. Apoi, spațiul gol care nu este gol — un modem 4G lăsat „pentru urgențe”, un laptop de mentenanță al furnizorului conectat la ambele rețele, un Wi-Fi activat din greșeală. Verificarea periodică a izolării, fizic, nu pe hârtie, face parte din tehnică.

Mai subtilă este erodarea prin comoditate. Prima excepție se face pentru un motiv bun; a cincea nu mai are motiv. Fiecare conexiune nouă spre un sistem izolat cere aprobare de la două persoane și o dată de expirare. Curierul însuși poate fi compromis, iar Convenția de la Viena protejează valiza de autorități, nu de curierul necinstit, așa că omul care traversează spațiul gol trebuie să fie, el însuși, verificat și supravegheat. Iar costul operațional este real — izolarea totală este scumpă în timp și oameni și se aplică la ceea ce este cu adevărat critic, nu la tot.

Cadrul legal

Art. 21 alin. (2) lit. (e) din Directiva NIS2 cere securitatea achiziției, dezvoltării și întreținerii sistemelor, iar lit. (i) controlul accesului și gestionarea activelor; pentru entitățile cu sisteme industriale sau medicale, izolarea acestora este cea mai directă măsură documentabilă. Art. 32 GDPR cere măsuri adecvate riscului, iar pentru datele sensibile, cele de sănătate de la art. 9, riscul justifică izolarea sistemelor care le prelucrează. În ISO/IEC 27001:2022, controalele A.8.22 (separarea rețelelor), A.7.10 (suporturi de stocare), A.8.12 (prevenirea scurgerilor de date) și A.8.31 (separarea mediilor de dezvoltare, testare și producție) acoperă toate formele acestei tehnici.

9. Blocul de unică folosință (one-time pad)



> **Într-o frază →** singura metodă de criptare dovedită matematic imposibil de spart — și lecția, plătită de serviciile sovietice, că nu algoritmul cedează, ci oamenii care gestionează cheile.

Epocă: 1917 → Războiul Rece · Amenințare: interceptarea comunicațiilor, gestionarea defectuoasă a cheilor, criptografia „făcută în casă" · Cost: zero (lecția) până la un sistem de gestionare a cheilor

Originea

În 1917, inginerul Gilbert Vernam, de la AT&T, a construit un dispozitiv care combina automat textul unui mesaj transmis prin teleimprimator cu o bandă perforată conținând o cheie, caracter cu caracter. Un ofițer al armatei americane, Joseph Mauborgne, a adăugat regula care transformă invenția într-o fortăreață. Cheia trebuie să fie *complet aleatoare*, cel puțin la fel de lungă ca mesajul, și *folosită o singură dată*. De aici numele, blocul (*pad*) de foi cu chei, din care fiecare foaie se rupe și se distruge după utilizare.

În 1949, Claude Shannon a demonstrat, în lucrarea *Communication Theory of Secrecy Systems*, ceea ce Mauborgne intuise. Un mesaj criptat astfel nu poate fi spart de nimeni, niciodată, cu nicio putere de calcul, pentru că textul cifrat este compatibil cu *orice* mesaj posibil de aceeași lungime. Fără cheie, nu există nicio informație de extras. Este singura schemă de criptare cu această proprietate. Tot ce folosim azi — AES, RSA, curbele eliptice — este „doar" foarte greu de spart; blocul de unică folosință este imposibil.

Cu această garanție, a devenit metoda aleasă pentru comunicațiile care nu-și permiteau niciun risc. Linia directă Moscova–Washington, instalată în 1963 după criza rachetelor din Cuba, nu era un telefon roșu, ci o legătură prin teleimprimator criptată cu benzi de unică folosință, schimbate prin curier diplomatic (fișa 8). Spionii sovietici și occidentali au purtat decenii întregi blocuri minuscule, tipărite pe hârtie care ardea instantaneu.

Și totuși, metoda imposibil de spart a fost spartă. Între 1943 și 1980, programul american VENONA a decriptat mii de mesaje sovietice din anii 1942–1945. Nu printr-o descoperire matematică, ci printr-o eroare de producție. Sub presiunea războiului, tipografia care producea blocurile pentru serviciile sovietice a dublat unele pagini, iar aceleași chei au fost trimise la mai multe ambasade. Două mesaje criptate cu aceeași cheie pot fi comparate, iar din comparație iese textul. Din VENONA au ieșit Klaus Fuchs, soții Rosenberg și o mare parte din rețeaua sovietică din Statele Unite. Algoritmul perfect fusese anulat de o imprimantă grăbită.

Surse: David Kahn, The Codebreakers (1996), cap. 13; Claude Shannon, „Communication Theory of Secrecy Systems”, Bell System Technical Journal, 1949; John Earl Haynes, Harvey Klehr, Venona (1999), cap. 1–2.

Principiul

Blocul de unică folosință învață două lucruri pe care orice organizație le ignoră pe rând.

Primul este că securitatea criptării stă în cheie, nu în algoritm. Algoritmii moderni sunt publici, verificați de mii de specialiști și, pentru scopuri practice, de nespart. Când criptarea eșuează, și eșuează des, este aproape întotdeauna pentru că cheia a fost reutilizată, generată prost, lăsată în cod, trimisă pe același canal cu mesajul sau păstrată lângă datele pe care le protejează. VENONA este, în esență, povestea fiecărei breșe de criptare de azi.

Al doilea este că o cheie are o durată de viață și o condiție de folosire, iar încălcarea lor anulează matematica. La blocul de unică folosință, condiția este absolută: o cheie, un mesaj, niciodată a doua oară. La cifrurile moderne, condiția este alta, dar la fel de strictă. O cheie AES poate cripta, legitim, milioane de mesaje; ceea ce nu se poate repeta este perechea cheie–nonce (valoarea unică adăugată fiecărei operații), iar în moduri precum AES-GCM reutilizarea aceluiași nonce cu aceeași cheie rupe confidențialitatea și autenticitatea în același fel în care paginile dublate au rupt VENONA. Iar la nivel uman, condiția se numește „o parolă, un serviciu”. Principiul comun este că secretul își pierde valoarea exact în momentul în care este folosit dincolo de condiția pentru care a fost proiectat.



Amenințarea de azi

Cea mai frecventă încălcare a principiului este banală, aceeași parolă pe mai multe servicii. Când un site oarecare este spart și lista de parole ajunge pe internet, atacatorii încearcă automat aceleași combinații de e-mail și parolă la toate băncile, la Microsoft 365, la Google. Tehnica se numește *credential stuffing* și funcționează pentru că oamenii fac, la scara lor, ceea ce a făcut tipografia din 1942. Folosesc același secret în două locuri.

A doua încălcare, mai tehnică, este criptografia improvizată. Dezvoltatori care „inventează" o schemă de criptare pentru aplicația lor, chei fixe scrise în codul sursă și publicate, odată cu el, pe GitHub, generatoare de numere aleatoare care nu sunt aleatoare. În 2022–2024, mai multe breșe majore au pornit de la chei de acces la servicii cloud lăsate în depozite publice de cod. Algoritmul era AES. Cheia era pe internet.

A treia este criptarea „sigură" ale cărei chei stau pe același server ca datele. Atacatorul care copiază baza de date copiază și cheia. Pentru notificarea încălcării, GDPR face diferența între date criptate și date în clar, dar numai dacă cheia nu a fost compromisă odată cu ele.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Cheia pe hârtie, în forma cea mai pură, arată așa. Pentru autorizarea plăților excepționale între director și contabil, o listă tipărită de 50 de coduri aleatoare, în două exemplare, fiecare cod folosit o singură dată și tăiat cu pixul după utilizare. Băncile românești au folosit exact acest sistem, listele TAN, ani de zile. Nu este un one-time pad în sens criptografic — nu criptează nimic —, ci disciplina lui aplicată unei singure întrebări: „chiar tu ai cerut plata asta?". Fiecare cod se folosește o dată și rezistă la clonarea vocii, la e-mail compromis și la deepfake, pentru că nu există nicăieri în format digital.

Pentru restul, un manager de parole pentru toată firma, cu o parolă diferită pentru fiecare serviciu, este cea mai eficientă măsură împotriva reutilizării parolelor la scară umană. Comunicațiile cu adevărat sensibile, cu avocatul, între asociați, despre o tranzacție, merg pe o aplicație cu criptare de la un capăt la altul, iar Signal este standardul, nu pe e-mail. Și nu inventați nimic. Orice program care promite „criptare proprietară" este un semnal de alarmă.

Firma de 500 de oameni

Cheile se gestionează centralizat, generate și păstrate într-un modul hardware de securitate sau într-un serviciu dedicat, separat de sistemele care le folosesc, cu rotație programată și cu jurnalizarea fiecărei utilizări. Codul sursă și depozitele se scanează automat pentru chei, parole și certificate lăsate în cod, înainte de fiecare publicare. Cheile de sesiune și certificatele au durată scurtă de viață și se reînnoiesc automat, fără nicio cheie „permanentă" în producție. Datele personale sensibile se criptează cu chei păstrate în alt sistem decât datele, astfel încât o copie a bazei de date să fie, singură, inutilă.

Unde eșuează

Reutilizarea, adică VENONA — la blocul de unică folosință, o cheie folosită de două ori este o cheie pierdută; la cifrurile moderne, echivalentul este nonce-ul repetat cu aceeași cheie, o greșeală de implementare mai frecventă decât pare. Aleatorul care nu este aleator — o cheie generată dintr-un algoritm previzibil sau dintr-o sursă slabă poate fi reconstituită, iar blocurile sovietice erau produse de dactilografe care, fiind oameni, nu băteau litere la întâmplare, un alt motiv pentru care VENONA a funcționat.

Distribuția cheii rămâne problema de fond. Blocul trebuie să ajungă la destinatar pe un canal sigur, și dacă acel canal există, de ce nu trimiți mesajul direct prin el? Răspunsul, că un curier este lent și rar, iar mesajele sunt dese, explică de ce blocul pur este rezervat pentru ce contează cel mai mult. Cheia lângă date este o încuietoare cu cheia în ușă. Iar perfecțiunea teoretică nu protejează metadatele — VENONA a identificat agenți și din tiparele de trafic, nu doar din conținut, iar cine vorbește cu cine, când și cât de des rămâne vizibil.

Cadrul legal

Art. 32 alin. (1) lit. (a) GDPR numește criptarea printre măsurile de securitate adecvate, iar art. 34 alin. (3) lit. (a) scutește operatorul de informarea persoanelor vizate dacă datele compromise erau criptate și cheia nu a fost accesată, ceea ce face gestionarea cheilor, nu criptarea în sine, criteriul decisiv. Art. 21 alin. (2) lit. (h) din Directiva NIS2 cere politici privind utilizarea criptografiei și, acolo unde este cazul, a criptării. În ISO/IEC 27001:2022, controlul A.8.24 cere reguli pentru utilizarea criptografiei și pentru întregul ciclu de viață al cheilor, de la generare și distribuție la stocare, rotație și distrugere, adică exact disciplina pe care tipografia din 1942 nu a avut-o.

10. Momeala



> **Într-o frază →** un lucru fals, atrăgător, pe care nimeni cinstit nu are motiv să-l atingă — astfel încât prima atingere este dovada că atacatorul a intrat.

Epocă: antichitate → 1986 · Amenințare: intruziuni nedetectate, scurgeri de date, mișcare laterală a atacatorilor · Cost: zero (instrumente gratuite)

Originea

În 217 î.Hr., Hannibal se afla prins în câmpia Falernului, cu armata lui Fabius Maximus ocupând singura trecătoare prin care putea ieși. Noaptea, a pus să se lege torțe aprinse de coarnele a două mii de boi și i-a mânat pe dealuri. Romanii de pe înălțimi au văzut ce păreau mii de soldați înaintând cu torțe spre o altă trecătoare, și-au părăsit poziția ca să o apere, iar Hannibal a trecut nestingherit prin cea rămasă liberă. Înșelarea era, în război, o armă a atacatorului. Apărătorul avea nevoie de aproape două mii de ani ca să o întoarcă în favoarea lui.

În 1930, firma americană de cartografie General Drafting a desenat pe harta statului New York un sat care nu exista, Agloe. Numele era un anagram al inițialelor proprietarilor, iar scopul era simplu — dacă o hartă concurentă avea să conțină Agloe, era dovada copierii. Când Rand McNally a publicat, ani mai târziu, o hartă cu Agloe pe ea, General Drafting a cerut socoteală. Tehnica, „străzile-capcană” și „orașele de hârtie”, a fost folosită de cartografi, de editorii de dicționare (enciclopedia *New Columbia* din 1975 conținea o fotografă inexistentă, Lillian Virginia Mountweazel) și de compilatorii de liste de adrese. O intrare falsă, unică, pe care doar cine copiază o poate avea. Nu împiedică furtul. Îl dovedește.

Apoi, în 1986, astronomul Clifford Stoll, administrator de sistem la laboratorul Lawrence Berkeley, a observat o diferență de 75 de cenți în contabilitatea timpului de

calculator. Urmărind-o, a descoperit un intrus care folosea sistemele laboratorului ca punte spre rețele militare. Pentru a-l ține conectat suficient de mult încât apelul să poată fi urmărit, Stoll a inventat un proiect inexistent, „SDINET”, cu dosare întregi de documente false și atrăgătoare despre Inițiativa de Apărare Strategică. Intrusul a petrecut ore citindu-le. Urmărirea a dus la Markus Hess, în Hanovra, care vindea informații KGB-ului. Cartea lui Stoll, *The Cuckoo's Egg*, a fost prima descriere publică a ceea ce azi se numește *honeypot*, borcanul cu miere.

Surse: Polibiu, Istorii, III, 93–94, pentru stratagema lui Hannibal; Mark Monmonier, How to Lie with Maps (1991), pentru străzile-capcană; Clifford Stoll, The Cuckoo's Egg (1989).

Principiul

Toate sistemele de detecție obișnuite au aceeași problemă. Trebuie să distingă activitatea legitimă de cea malițioasă într-un ocean de activitate legitimă, iar rezultatul sunt alarme false, oboseală și, în cele din urmă, ignorarea alarmelor.

Momeala ocolește problema prin construcție. **Un obiect pe care nimeni nu are motiv legitim să-l atingă produce alerte cu un grad foarte ridicat de încredere.** Orice interacțiune cu el este, aproape prin definiție, suspectă — rămân doar accidentele, cum ar fi angajatul curios, iar acestea se verifică într-un minut. Prima atingere este un indicator care cere investigație imediată, nu dovada certă a unei intruziuni; diferența față de alertele obișnuite este că aici investigația merită aproape întotdeauna efortul. Nu e nevoie de analiză, de euristici, de învățare automată, ci doar de un obiect atrăgător și de un fir care sună când este atins.

Momeala ia trei forme. Momeala-obiect, *honeytoken*, este un fișier, o înregistrare, un cont sau o cheie care nu are nicio funcție, dar arată valoros — „parole_directori.xlsx”, un client inexistent în baza de date, un cont de administrator pe care nu-l folosește nimeni. Momeala-sistem, *honeypot*, este un server fals, cu porturi deschise și servicii aparent vulnerabile, care nu face nimic decât să înregistreze cine încearcă să intre. Iar momeala-marcaj, strada-capcană, este o intrare unică plasată în fiecare copie a unui set de date, care identifică de unde a plecat o scurgere.



Amenințarea de azi

Timpul mediu între intrarea unui atacator într-o rețea și descoperirea lui s-a măsurat, ani la rând, în luni. Atacatorii de ransomware petrec zile sau săptămâni explorând rețeaua, căutând copiile de rezervă (fișa 5), parolele salvate, serverele de fișiere. În toată această perioadă, firma nu știe nimic. Fiecare zi de nedetectare înseamnă mai multe date exfiltrate și mai puține copii de rezervă rămase.

Un atacator care explorează o rețea face exact ceea ce a făcut Markus Hess. Deschide dosare, caută fișiere cu nume interesante, încearcă parole pe servere. Dacă, printre dosarele reale, există câteva false, cu fir, atacatorul va deschide unul în primele ore, nu pentru că este neglijent, ci pentru că nu are cum să știe care este fals.

A doua problemă este scurgerea de date. Lista de clienți ajunge la concurență, baza de date a unui furnizor apare pe un forum. Întrebarea „de unde a plecat?" este, de obicei, fără răspuns, pentru că toate copiile sunt identice. Strada-capcană răspunde. Dacă fiecare copie trimisă unui partener conține un client fictiv diferit, cu o adresă de e-mail unică, primul mesaj primit pe acea adresă spune exact care partener a pierdut lista.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Serviciul Canarytokens (canarytokens.org, gratuit, oferit de o firmă de securitate) generează documente Word, PDF și Excel care trimit o alertă pe e-mail în momentul în care sunt deschise, oriunde în lume — cu o rezervă: alerta depinde de aplicația care deschide fișierul, iar unele cititoare de PDF sau previzualizări nu o declanșează, deci testați fiecare momeală cu programele folosite în firmă înainte de a vă baza pe ea. Puneți trei-patru astfel de fișiere, cu nume atrăgătoare, în dosarele partajate, „Salarii 2026.xlsx", „Parole servere.docx", „Contract vânzare firmă.pdf". Nimeni din firmă nu are motiv să le deschidă; spuneți-le oamenilor că există, fără să spuneți care sunt.

Creați un cont de utilizator fals în domeniu, cu nume plauzibil și parolă complexă, pe care nimeni nu-l folosește, și configurați o alertă la orice încercare de autentificare pe el — în Windows, printr-o regulă simplă pe jurnalul de securitate, sau prin instrumentul de monitorizare pe care îl aveți. În baza de date de clienți, adăugați

două-trei intrări fictive, cu adrese de e-mail create special. Orice mesaj primit pe ele este dovada că lista a ieșit din firmă.

Firma de 500 de oameni

Momelile se distribuie sistematic — fișiere-capcană pe fiecare server de fișiere, conturi-capcană în fiecare domeniu, chei de acces false în depozitele de cod și în configurații, pentru că un atacator care găsește o cheie de cloud o va încerca în minute. Un honeypot intern, un server care imită un sistem interesant precum o consolă de backup sau un server de baze de date, se plasează în segmentele unde atacatorul ar ajunge după primul compromis, iar orice conexiune la el este un incident de prioritate maximă.

Seturile de date trimise partenerilor și furnizorilor se marchează cu înregistrări unice per destinatar, documentat în contract. Alertele de pe momeli ocolesc fluxul obișnuit de triaj și ajung direct la echipa de răspuns, pentru că sunt rareori false și, când sunt, se lămuresc repede.

Unde eșuează

Momeala prea evidentă nu prinde pe nimeni. Un fișier numit „HONEYPOT – NU DESCHIDE” este decor; momeala trebuie să arate ca restul. Momeala uitată produce alerta falsă tipică a tehnicii — documentul-capcană din 2024 este deschis de noul angajat care face ordine în dosare, iar dacă se repetă, se pierde încrederea în alarme. Lista momelilor se ține la zi, în plicul sigilat din fișa 4.

Alerta pe care nu o citește nimeni este eșecul clasic, cu firul care sună într-o căsuță de e-mail pe care nu o verifică nimeni. Alerta trebuie să ajungă la o persoană, pe telefon, cu procedura din fișa 3 lângă ea. Atacatorul precaut, din grupurile sofisticate, știe că există momeli și le evită, dar chiar și pentru el momeala este utilă, pentru că îl încetinește și îl obligă la o prudență care produce alte urme.

Rămâne problema juridică. Un honeypot care *atrage activ* atacatori din exterior, de exemplu pe internet, ridică întrebări de drept penal și de protecția datelor celor care îl ating. Momelile interne, pe sistemele proprii, nu au această problemă; cele externe cer consultarea unui jurist.

Cadrul legal

Art. 21 alin. (2) lit. (b) din Directiva NIS2 cere gestionarea incidentelor, ceea ce presupune detectarea lor; art. 23 impune termene de notificare care curg de la momentul în care entitatea „ia cunoștință” de incident, iar fără detecție termenele nu pot fi respectate. Sub GDPR, art. 33 cere notificarea în 72 de ore de la luarea la cunoștință, iar art. 32 cere capacitatea de a evalua periodic eficacitatea măsurilor; un atacator care circulă nedetectat luni de zile este o dovadă de ineficacitate. În ISO/IEC 27001:2022, controlul A.8.16 (activități de monitorizare) cere detectarea comportamentului anormal, iar A.5.24–A.5.26 gestionarea și evaluarea evenimentelor de securitate.

11. Codul de constrângere



> **Într-o frază →** un semnal convenit dinainte, invizibil pentru cel care te forțează, prin care transmiți „fac ce mi se cere, dar nu de bunăvoie” — ca apoi cineva să acționeze.

Epocă: Al Doilea Război Mondial → Războiul din Vietnam · Amenințare: coerciție fizică sau psihologică a unui angajat, jaf, răpire, șantaj, „insider” forțat · Cost: zero

Originea

Agenții serviciului britanic SOE parașutați în Europa ocupată transmiteau prin radio mesaje criptate către Londra. Fiecare operator avea două „verificări de securitate” convenite înainte de plecare. *Bluff check* era o eroare deliberată pe care, dacă era capturat și forțat să transmită, o putea „mărturisi” nemților ca fiind semnalul secret. *True check* era a doua eroare, cea adevărată, de exemplu litera greșită la fiecare al optsprezecelea caracter. Un mesaj fără *true check* însemna un singur lucru — operatorul transmite sub control inamic.

În martie 1942, operatorul olandez Huub Lauwers a fost capturat de Abwehr la Haga. Forțat să transmită, a omis verificarea adevărată, exact cum fusese instruit. Londra a răspuns, i-a reproșat că a uitat verificarea și a continuat să-i trimită instrucțiuni, bani și agenți. Timp de doi ani, în ceea ce germanii au numit *Englandspiel*, „jocul Angliei”, serviciul de contraspionaj german a controlat aproape toată rețeaua SOE din Olanda, primind peste cincizeci de agenți direct în brațele lor la aterizare. Majoritatea au murit în lagăre. Codul de constrângere a funcționat perfect. Nu a funcționat cel care trebuia să-l citească.

În 1966, comandorul american Jeremiah Denton, prizonier în Vietnamul de Nord, a fost adus în fața camerelor pentru un interviu de propagandă. În timp ce spunea, obligat, că este tratat bine, a clipit în cod Morse T-O-R-T-U-R-E. Înregistrarea a fost

difuzată în Statele Unite și a fost prima confirmare că prizonierii americani erau torturați. Nimeni nu convenise semnalul; Denton a mizat pe faptul că cineva, undeva, știa Morse și se uita atent. De data aceasta, cineva s-a uitat.

Surse: Leo Marks, Between Silk and Cyanide (1998), cap. despre Olanda; M. R. D. Foot, SOE in the Low Countries (2001); Jeremiah Denton, When Hell Was in Session (1976).

Principiul

Toate celelalte tehnici din acest catalog presupun că persoana autorizată acționează liber. Codul de constrângere acoperă cazul în care nu o face — angajatul cu un cuțit la gât, contabilul șantajat, administratorul IT amenințat cu publicarea unor fotografii, directorul a cărui familie este reținută.

În aceste situații, refuzul este periculos, iar cooperarea aparentă este singura opțiune. Codul de constrângere oferă un al treilea canal. Acțiunea cerută se execută, sau pare că se execută, dar lângă ea trece un semnal pe care atacatorul nu-l vede, iar cineva din afară știe că trebuie să intervină.

Ca să funcționeze, semnalul trebuie să fie indistinctibil de normalitate pentru cineva care nu-l cunoaște, adică o eroare, o frază obișnuită sau un cod diferit de cel uzual, dar care funcționează. Receptorul trebuie să fie instruit să-l recunoască și să aibă o procedură, iar Englandspiel este eșecul exact al acestei condiții. Iar atacatorul nu trebuie să poată verifica dacă semnalul a fost transmis sau nu.



Amenințarea de azi

Coerciția nu a dispărut odată cu digitalizarea; și-a schimbat forma. Grupurile de infractori cibernetici recrutează sau șantajează angajați cu acces. În 2020, un cetățean rus a încercat să ofere unui angajat Tesla un milion de dolari pentru a instala malware în rețeaua fabricii din Nevada; angajatul a raportat tentativa, iar FBI-ul a intervenit. Nu toate cazurile se termină așa, iar multe nu se află niciodată, pentru că angajatul constrâns a executat, iar firma a tratat incidentul ca pe un atac extern.

Jaful clasic a devenit hibrid, cu amenințarea fizică a unui angajat pentru a obține acces la sisteme, la seif sau la conturi. Iar răpirile-fulger cu scopul de a forța transferuri

bancare sau de criptomonede de pe telefonul victimei, cunoscute în Franța, Spania și America Latină, au apărut și în Europa de Est.

În toate aceste situații, politicile obișnuite de securitate sunt neputincioase. Persoana are credențiale valide, acțiunea este autorizată, parola de recunoaștere (fișa 1) este cunoscută. Singurul lucru care diferă este că persoana nu vrea să o facă, și nimic din sistem nu are cum să vadă asta, decât dacă a fost construit special pentru.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Începeți cu sistemul de alarmă. Aproape orice centrală permite un cod de constrângere, diferit de cel obișnuit, care dezarmează sistemul normal, dar trimite o alertă silențioasă la firma de pază. Dacă aveți pază, activați-l și asigurați-vă că dispeceratul știe ce înseamnă. Dacă nu l-ați configurat niciodată, aceasta este sarcina de luni.

Apoi fraza de constrângere verbală. Conveniți, împreună cu parola de recunoaștere din fișa 1, o frază aparent banală care înseamnă „sunt forțat” — nu un cuvânt ciudat, ci ceva ce se poate strecura natural, de exemplu „trimite-mi și situația de la Brașov”, când firma nu are nimic la Brașov. Cel care o aude confirmă calm, tergiversează („durează vreo oră, te sun eu”) și sună la 112. Procedura pentru receptor, adică ce face exact persoana care primește semnalul, se scrie în runbook (fișa 3); fără procedură, aveți un Englandspiel. Discutați tehnica și cu familia, pentru apelurile de tip „am nevoie de bani acum”.

Firma de 500 de oameni

Codul de constrângere se configurează pe toate sistemele de control al accesului fizic, uși, seifuri, camere de servere, și pe sistemul de alarmă, cu testarea trimestrială a răspunsului dispeceratului. Pentru personalul cu acces privilegiat și pentru cei care pot autoriza plăți mari se stabilește, la instruire, o frază de constrângere individuală, cunoscută de echipa de securitate. Un mecanism tehnic complementar este aprobarea „întârziată” a tranzacțiilor excepționale, care cere o confirmare suplimentară după o oră, din alt loc, timp în care o persoană constrânsă poate ajunge în siguranță.

Directorii care călătoresc în zone cu risc au o procedură de *proof of life*, convenită cu familia și cu firma. Iar angajații sunt instruiți explicit că raportarea unei tentative de recrutare sau șantaj este protejată și recompensată, nu sancționată — cazul Tesla a fost posibil pentru că angajatul a avut încredere că poate raporta.

Unde eșuează

Cel mai grav mod de eșec este receptorul care nu știe, Englandspiel. Semnalul este trimis corect și ignorat, iar instruirea receptorului contează mai mult decât semnalul. Apoi este atacatorul care știe că există coduri de constrângere. Un infractor pregătit va întreba „care e codul de constrângere?” și va cere codul normal, de aceea codul de

constrângere trebuie să *funcționeze* vizibil — ușa se deschide, seiful se deblochează — astfel încât atacatorul să nu poată distinge între cele două.

Uitarea sub stres este reală. Oamenii uită, sub amenințare, lucruri pe care le știu perfect, așa că semnalul trebuie să fie simplu și exersat, pentru că o frază lungă nu va fi rostită. Alarma falsă, când cineva folosește codul din greșeală, cere ca procedura să prevadă și verificarea discretă înainte de intervenția în forță.

Și un mit, cel al PIN-ului inversat. Circulă de ani de zile ideea că introducerea PIN-ului în ordine inversă la bancomat alertează poliția. Nu există un asemenea sistem. Codurile de constrângere trebuie configurate explicit; nu vin de la sine.

Cadrul legal

Art. 21 alin. (1) din Directiva NIS2 cere măsuri care să protejeze inclusiv mediul fizic al sistemelor, iar alin. (2) lit. (i) politici de securitate a resurselor umane și de control al accesului. Sub GDPR, art. 32 nu distinge între accesul neautorizat obținut prin exploatarea unei vulnerabilități și cel obținut prin constrângerea unui angajat, iar operatorul răspunde pentru ambele. În ISO/IEC 27001:2022, controalele A.7.1–A.7.4 (securitatea fizică și monitorizarea), A.6.3 (instruirea personalului) și A.6.8 (raportarea evenimentelor de securitate) acoperă implementarea; legislația națională privind paza obiectivelor și cea privind sistemele de alarmă completează cadrul.

12. Jurnalul santinelei



> **Într-o frază →** nu este suficient ca cineva să stea de pază — trebuie să existe dovada că a stat, cineva care verifică dovada și o consecință când lipsește; paza fără jurnal este o speranță.

Epocă: Roma republicană → marina cu pânze · Amenințare: intruziuni nedetectate, ștergerea urmelor de către atacatori, imposibilitatea de a reconstitui ce s-a întâmplat · Cost: zero până la un serviciu de monitorizare

Originea

Polibiu, în aceeași carte a VI-a a *Istoriilor* în care descrie parola zilnică (fișa 1), explică și cum se asigurau romanii că santinelele chiar stau de pază. Fiecare post de gardă din tabără primea, la începutul nopții, o tăbliță mică de lemn cu un semn. Noaptea era împărțită în patru schimburi, și în fiecare schimb patru călăreți făceau rondul posturilor. La fiecare post, santinela trebuia să-i predea tăblița; dacă rondul o găsea dormind sau lipsă, nu lua tăblița, ci chema martori. Dimineața, tăblițele erau predate tribunului. Dacă lipsea una, se știa exact care post și care schimb, iar santinela vinovată era judecată și, de regulă, bătută cu bețe de propriii camarazi, de obicei până la moarte. Polibiu notează, cu o anume admirație, că din această cauză străjile de noapte ale romanilor erau de o rigoare impecabilă.

Sistemul are patru componente și toate patru contează — paza, adică santinela; dovada, adică tăblița; verificarea, adică rondul și tribunul; și consecința, adică pedeapsa. Scoateți oricare dintre ele și celelalte trei devin teatru.

Marina a adăugat a doua idee, jurnalul de bord. Pe orice navă, ofițerul de cart consemnează, la intervale fixe, poziția, cursul, vântul, vremea, orice vas întâlnit și orice eveniment. Nu pentru că i-ar folosi lui în acel moment, ci pentru că, dacă nava se scufundă, jurnalul este singurul martor, și pentru că, în caz de litigiu, un jurnal ținut

regulat este probă în instanță, iar unul cu pagini lipsă este probă împotriva celui care l-a ținut. Jurnalul Titanicului s-a scufundat cu nava, dar cel al navei Californian, aflată în apropiere, a fost citit rând cu rând în anchetă, inclusiv orele la care fuseseră observate rachetele de semnalizare, fără ca cineva să acționeze.

La începutul secolului XX, paznicii de noapte ai fabricilor primeau un „ceas de rond", un dispozitiv purtat la brâu, în care se introduceau, în ordine, chei fixate pe ziduri în diferite puncte ale clădirii; fiecare cheie imprima ora pe o bandă de hârtie sigilată în interior. Dimineața, patronul deschidea ceasul și vedea dacă paznicul a trecut pe la toate punctele și la ce ore. Tăblița lui Polibiu, cu mecanism de ceasornic.

Surse: Polibiu, Istorii, VI, 35–37; British Wreck Commissioner's Inquiry (1912), depozițiile ofițerilor navei Californian; cataloagele de ceasuri de rond Detex/Bürk, începutul secolului XX.

Principiul

Un sistem informatic produce, în fiecare secundă, mii de înregistrări despre ce se întâmplă în el — cine s-a autentificat, de unde, ce a deschis, ce a schimbat, ce a eșuat. Acestea sunt tăblițele santinelelor. Majoritatea organizațiilor le lasă să se acumuleze și să se suprascrie, pe aceleași mașini pe care le descriu, fără să le citească nimeni. Au santinela și tăblița. Nu au rondul, tribunul și consecința.

Jurnalul santinelei cere patru lucruri. Înregistrarea evenimentelor care contează, cu ora exactă, ceea ce înseamnă că sistemele trebuie să aibă ceasul sincronizat, altfel reconstituirea devine un exercițiu de ghicit. Păstrarea înregistrărilor în alt loc decât sistemul care le produce, pentru ca un atacator care controlează sistemul să nu poată șterge dovada că l-a controlat. Verificarea periodică, de către cineva, a înregistrărilor critice, adică rondul. Și reacția la ce se găsește, adică consecința.



Amenințarea de azi

Unul dintre primele lucruri pe care le fac mulți atacatori după ce obțin drepturi de administrator pe o mașină Windows este să șteargă jurnalele de evenimente. Comanda are o singură linie. Apoi dezactivează jurnalizarea. Când firma descoperă atacul, săptămâni mai târziu, nu mai există nimic de citit — nu se știe când a intrat, pe

unde, ce a copiat, câte sisteme a atins. Notificarea către ANSPDCP trebuie să descrie natura încălcării și categoriile de date afectate; fără jurnale, singura descriere onestă este „nu știm”, iar legea nu acceptă „nu știm” ca răspuns.

Al doilea scenariu este cel al jurnalului care există și pe care nimeni nu l-a citit. Într-un număr mare de incidente investigate, urmele atacatorului erau în jurnale cu zile sau săptămâni înainte de criptare — autentificări reușite la ore imposibile, din țări în care firma nu are angajați, crearea unui cont de administrator nou, dezactivarea antivirusului, modificarea politicii de retenție a copiilor de rezervă (fișa 5). Fiecare dintre acestea era tăblița lipsă pe care rondul ar fi observat-o. Nu exista rond.

Nava Californian a văzut rachetele. Jurnalul a consemnat ora. Nimeni nu a trezit căpitanul.

Cum o implementezi luni dimineață

Firma de 20 de oameni

Alegeți cele șase evenimente care contează și configurați alerte doar pentru ele — autentificare reușită în contul de administrator, crearea unui cont nou, adăugarea unui cont în grupul de administratori, dezactivarea protecției antivirus, modificarea sau ștergerea sarcinilor de backup și autentificare reușită din afara țării pe Microsoft 365 sau Google Workspace. Toate pot fi configurate gratuit în instrumentele pe care le aveți deja, iar alertele vin pe e-mail sau pe telefon.

Jurnalele serverului se trimit automat pe un al doilea sistem, care poate fi un calculator vechi, un NAS sau un serviciu gratuit în cloud, cu credențiale diferite de cele ale domeniului. Cât timp le păstrați decideți în funcție de risc și de obligațiile care vi se aplică; pentru o firmă mică, 12 luni este un punct de plecare rezonabil, pentru că atacatorii stau în rețea săptămâni sau luni înainte de a lovi. Sincronizați ceasul tuturor sistemelor cu o sursă de timp de pe internet; este o setare, nu un proiect.

Rondul arată așa. Cineva, în fiecare luni, 15 minute, se uită la lista autentificărilor din săptămâna trecută și la alertele primite, și consemnează într-un rând data, cine, „nimic suspect” sau ce s-a găsit. Rândul acela este tăblița predată tribunului.

Firma de 500 de oameni

Jurnalele se centralizează într-un sistem dedicat (SIEM), cu înlănțuire criptografică a înregistrărilor (fișa 7), pe o infrastructură cu credențiale complet separate; perioada de retenție se stabilește din analiza de risc și din cerințele sectoriale aplicabile, iar 12–24 de luni este intervalul pe care îl întâlnim cel mai des în practică. Monitorizarea este continuă, internă sau printr-un furnizor de detecție și răspuns, cu reguli definite pentru tiparele cunoscute de atac, nu pentru „tot”, ci pentru ce contează. Pentru datele personale sensibile — sănătate, salarii, evaluări — granularitatea jurnalizării se decide proporțional cu riscul: acolo unde o plângere sau un incident ar cere să dovediți cine a deschis un anumit dosar și când, jurnalizarea la nivel de înregistrare este singura dovadă posibilă, și tot ea este cea care vă permite să demonstrați că accesul s-a limitat la necesar.

Jurnalizarea se testează periodic printr-un exercițiu în care un membru al echipei face o acțiune care *ar trebui* să producă o alertă și se măsoară dacă și când ajunge alerta la cineva. Rondul verifică santinela; cineva trebuie să verifice și rondul.

Unde eșuează

Jurnalul pe aceeași mașină este eșecul fundamental. Dacă atacatorul controlează sistemul, controlează și dovada, iar cel mai important pas este mutarea jurnalelor în altă parte, înainte de orice altceva. Zgomotul vine imediat după — jurnalizarea a tot produce milioane de rânduri pe care nu le citește nimeni și în care alarmele reale se înecă. Începeți cu șase evenimente și adăugați altele doar când cele șase sunt verificate săptămânal.

Rondul formal este tăblița predată fără ca cineva să se fi uitat la post. Verificarea săptămânală trebuie să fie reală și consemnată, iar în audit rândul lipsă este dovada că nu a existat. Lipsa consecinței golește tot restul de sens. Romanii aveau o pedeapsă brutală și, prin urmare, străji impecabile; organizațiile nu au nevoie de brutalitate, dar au nevoie de consecință, pentru că alerta ignorată trebuie să aibă un răspuns, altfel următoarea va fi ignorată și ea.

Retenția scurtă, jurnale de 30 de zile pentru un atacator care a stat 60, se rezolvă stabilind perioada din risc, nu din spațiul de pe disc. Iar ceasul nesincronizat face din reconstituirea unui atac, cu două sisteme cu ore diferite, un exercițiu de ghicit.

Cadrul legal

Art. 5 alin. (2) GDPR (responsabilitatea) cere operatorului să poată *demonstra* conformitatea, iar art. 33 alin. (3) cere ca notificarea unei încălcări să descrie natura ei, categoriile și numărul aproximativ de persoane și înregistrări afectate, informații care nu există fără jurnale; art. 33 alin. (5) impune documentarea fiecărei încălcări, inclusiv a celor nenotificate. Art. 21 alin. (2) lit. (b) din Directiva NIS2 cere gestionarea incidentelor, iar lit. (f) politici și proceduri de evaluare a eficacității măsurilor de securitate, iar jurnalul verificat este dovada standard a amândurora. În ISO/IEC 27001:2022, controalele A.8.15 (jurnalizare), A.8.16 (monitorizare) și A.8.17 (sincronizarea ceasurilor) sunt, împreună, sistemul lui Polibiu.

Plan de acțiune: prima zi, prima săptămână, prima lună

Fișele explică fiecare tehnică în parte. Această pagină le pune în ordine, pentru cititorul care răspunde de o organizație și vrea să știe de unde începe luni dimineață, cine face ce și cum dovedește, peste trei luni, că s-a făcut. Ordinea nu este după importanță, ci după raportul dintre efect și efort — primele măsuri costă nimic și închid frauda cea mai frecventă; ultimele cer un proiect.

Costurile și eforturile din tabele sunt orientative, pentru o firmă mică; depind de capacitatea de stocare necesară, de numărul de utilizatori și de timpul oamenilor voștri, care este, de regulă, costul cel mai mare și cel mai ușor de ignorat. Planul este scris pentru o firmă de 20–100 de oameni, fără departament de securitate. Pentru o organizație mai mare, aceleași rânduri devin cerințe pentru echipa IT și pentru furnizorul de servicii, cu aceleași dovezi. Nu este un plan de conformitate; este un plan de reducere a riscurilor celor mai frecvente, din care documentația de conformitate are ce prelua.

Prima zi

Măsura	Fișa	Cine	Efort	Dovada
Convenirea cuvântului de verificare între cei care aprobă plăți și acces	1	Directorul, cu 3–5 persoane, față în față	30 min	O linie în procedura de plăți: „cererile prin telefon/mesaj se verifică prin cuvânt și apel de confirmare” (fără cuvânt)
Activarea dublei semnături pe conturile bancare, peste un prag	2	Directorul, în aplicația băncii	30 min	Captura setării din aplicația băncii, cu pragul
Regula IBAN-ului nou: nicio schimbare de cont fără apel la numărul din contract	7	Contabilitatea	15 min	Lista tipărită a IBAN-urilor furnizorilor recurenți, semnată și datată
Lista de telefoane pentru incident, pe hârtie, în două exemplare	3	Directorul	1 oră	Prima pagină a dosarului de incident, datată
Verificarea că există o copie de rezervă validă (un fișier restaurat de probă) și, abia apoi, scoaterea discului de backup din USB între rulări	5	IT	30 min	Fișa de test cu data și fișierul restaurat (rotația, în săptămâna 1)

Prima săptămână

Măsura	Fișa	Cine	Efort	Dovada
Dosarul de incident complet: primele 10 acțiuni, criteriile de evaluare și notificare, unde sunt copiile, jurnal gol	3	Directorul + IT + DPO	½ zi	Dosarul tipărit, cu data pe copertă; locul lui cunoscut de echipa de criză
Două discuri externe în rotație săptămânală, unul mereu deconectat și în altă clădire; backup zilnic criptat, cu confirmarea că rulează și după rotație	5	IT	2 ore + discurile (prețul depinde de capacitate)	Calendarul rotației; parola copiei în plic sigilat; raportul primei rulări

Măsura	Fișa	Cine	Efort	Dovada
Secretele de urgență scrise de mână și sigilate; registrul sigiliilor	4	IT + directorul	1 oră + 20–50 lei	Registrul cu numărul sigiliului, data, semnăturile
Conturi de administrator separate de conturile de lucru; MFA pe toate conturile cu acces la bani, e-mail și sisteme	2, 6	IT	½ zi	Lista conturilor privilegiate; raportul MFA din consola de administrare
Codul de constrângere activat la alarmă; fraza de constrângere convenită odată cu cuvântul de verificare	11	Directorul + firma de pază	1 oră	Confirmarea scrisă a dispeceratului că știe ce înseamnă codul
Cele șase alerte care contează, configurate (admin, cont nou, grup admin, antivirus oprit, backup modificat, autentificare din altă țară)	12	IT	2 ore	Captura regulilor de alertă; un test cu o alertă provocată

Prima lună

Măsura	Fișa	Cine	Efort	Dovada
Tabelul accese actuale / accese necesare și curățarea diferenței; dosarul unic partajat împărțit pe departamente	6	Fiecare manager + IT	1–2 zile	Tabelul semnat de manageri; structura nouă de drepturi
Rețeaua de oaspeți, imprimantele și camerele pe segment separat; închiderea accesului de la distanță nefolosit	6, 8	IT	½ zi	Configurația routerului; lista porturilor expuse, verificată din exterior
Laptop dedicat pentru bancă și semnături electronice	8	IT	2 ore + un laptop (orientativ, cât un laptop de birou obișnuit)	Inventarul: un echipament, un singur scop
Trei–patru documente-momeală în dosarele partajate; un cont-momeală în domeniu	10	IT	1 oră	Lista momelilor în plicul sigilat; o alertă de test
Jurnalele trimise pe un al doilea sistem, cu credențiale separate; ceasurile sincronizate	12	IT	½ zi	Captura configurației; un rând în registrul rondului săptămânal
Primul test de restaurare: un fișier la întâmplare, de pe discul deconectat, pe alt calculator, cu timp măsurat	5	IT, cu directorul de față	30 min	Fișa de test: data, fișierul, timpul, rezultatul
Primul exercițiu pe masă: se deschide dosarul de incident și se parcurg pașii cu ceasul în mână	3	Echipa de criză	2 ore	Lista a ce nu a mers, cu termene
Manager de parole pentru toată firma; semnătură electronică calificată pentru cei care semnează contracte	9, 7	IT + directorul	½ zi + abonamente anuale (manager de parole per utilizator, certificat calificat per semnatar)	Lista utilizatorilor; certificatele emise

Ce se repetă

Planul de mai sus se face o dată. Ce îl ține în viață este un calendar scurt, cu rânduri care se bifează și se semnează — acesta este, de altfel, jurnalul santinelei aplicat propriilor voastre măsuri.

Ritm	Ce	Fișa
Săptămânal	Rondul de 15 minute pe autentificări și alerte; rotația discului de backup	12, 5
Lunar	Un test de restaurare; verificarea că alertele încă ajung la cineva	5, 12
Trimestrial	Verificarea sigiliilor; revizuirea listei de accese cu fiecare manager; schimbarea cuvântului de verificare; verificarea numerelor din dosarul de incident; testul codului de constrângere cu dispeceratul	4, 6, 1, 3, 11
Semestrial	Exercițiul pe masă; testul de restaurare completă a unui sistem critic	3, 5
La fiecare plecare din firmă	Dezactivarea conturilor în aceeași zi; schimbarea cuvântului de verificare dacă persoana îl știa; plic nou dacă persoana cunoștea un secret de urgență	6, 1, 4

Dovezile din coloana din dreapta nu sunt birocrație. Sunt exact documentele pe care le va cere un auditor, un asigurator după un incident sau autoritatea de supraveghere după o notificare — și, mai important, sunt singurul mod în care veți ști, peste un an, că măsurile încă există, nu doar că au existat.

Mituri: unde „vechiul” nu te salvează



O carte care laudă tehnicile vechi are datoria să spună și unde ele nu funcționează — sau unde credința că funcționează este, ea însăși, o vulnerabilitate. Cele cinci mituri de mai jos sunt cele pe care le aud cel mai des, în ordinea în care produc pagube.

Mitul 1: „Trecem pe mașini de scris și nu ne mai poate spiona nimeni”

În 2013, după dezvăluirile despre supravegherea americană, Serviciul Federal de Pază al Rusiei a comandat mașini de scris electrice pentru documentele cele mai sensibile; un deputat german a sugerat public același lucru pentru comisia de anchetă a Bundestagului. Ideea are o logică reală — un document care nu a existat niciodată în format digital nu poate fi exfiltrat prin rețea — și o istorie care o contrazice.

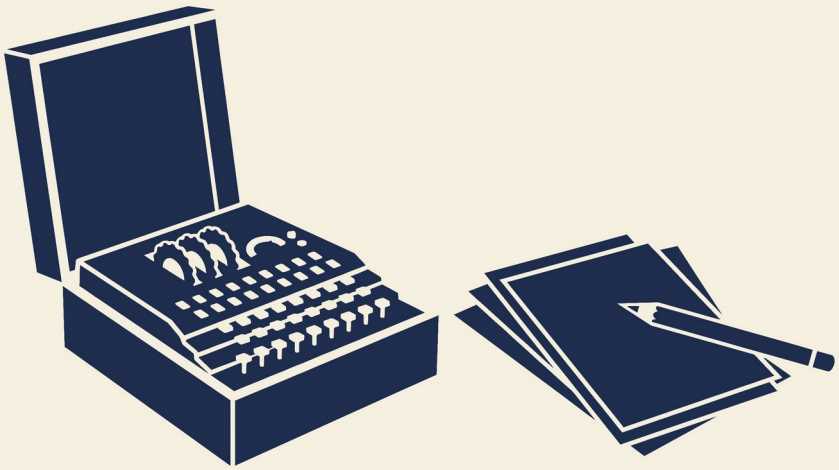
Între 1976 și 1984, serviciile sovietice au instalat dispozitive de ascultare în șaisprezece mașini de scris IBM Selectric din ambasada americană de la Moscova. Dispozitivele, ascunse într-o bară metalică a mașinii, înregistrau mișcarea capului de scris și transmiteau prin radio fiecare literă bătută. Au fost descoperite abia în 1984, în cadrul operațiunii americane GUNMAN, după ce un aliat a semnalat o problemă similară. Timp de opt ani, documentele „sigure”, bătute la mașină tocmai pentru a nu trece prin sistemele electronice, au fost citite în timp real de adversar.

La o scară mai mică: panglica unei mașini de scris păstrează, lizibil, tot ce s-a scris cu ea; caracterele fiecărei mașini au imperfecțiuni unice, folosite de criminalistică de un secol pentru a identifica mașina sursă; iar o foaie bătută la mașină se fotocopiază, se fotografiază și se fură exact ca orice foaie.

Mașina de scris elimină o categorie de atacuri (cele prin rețea) și lasă intacte toate celelalte (fizice, prin emanații, prin oameni). Nu este o măsură de securitate; este o

mutare a suprafeței de atac din locul în care ați învățat s-o apărați în locul în care ați uitat.

Surse: NSA, Learning from the Enemy: The GUNMAN Project (2007, desecretizat); Reuters, 11 iulie 2013, pentru comanda FSO.



Mitul 2: „Enigma era de nespart; au avut noroc”

Mașina Enigma a fost, pentru vremea ei, o realizare criptografică remarcabilă, iar spargerea ei la Bletchley Park este una dintre marile povești ale secolului XX. Dar Enigma nu a fost spartă pentru că matematicienii aliați au fost geniali — deși au fost. A fost spartă pentru că operatorii germani au fost oameni.

Matematicienii polonezi conduși de Marian Rejewski au pătruns în sistem încă din 1932, exploatând o slăbiciune de *procedură*: cheia de mesaj era transmisă de două ori la începutul fiecărui mesaj, ceea ce crea un tipar. La Bletchley, „bombele” lui Turing căutau fragmente de text cunoscut (*cribs*): operatorii începeau mesajele cu formule previzibile, buletinele meteo aveau aceeași structură în fiecare zi, unii încheiau cu „Heil Hitler”. Operatori leneși alegeau setări de rotoare ușor de ghicit, iar o particularitate a mașinii — o literă nu putea fi niciodată criptată în ea însăși — reducea drastic spațiul de căutare. Cărțile de coduri capturate de pe submarine au făcut restul.

Lecția nu este că Enigma era slabă. Este că niciun algoritm nu rezistă la procedură proastă, la reutilizare și la oameni grăbiți — exact ce arată și blocul de unică folosință din fișa 9. Când cineva vă spune că sistemul lui este „de nespart”, întrebați cum sunt instruiți operatorii.

Mitul 3: „Dacă nu știe nimeni cum funcționează, e sigur”

În 1883, criptograful olandez Auguste Kerckhoffs a formulat principiul care îi poartă numele: un sistem criptografic trebuie să fie sigur chiar dacă totul despre el, cu excepția cheii, este cunoscut de adversar. Claude Shannon l-a reformulat mai simplu: *presupune că inamicul cunoaște sistemul*.

Securitatea prin obscuritate — portul „ascuns”, aplicația „pe care nu o știe nimeni”, algoritmul proprietar — funcționează exact până în momentul în care cineva află, și acel moment vine întotdeauna: un angajat pleacă, un furnizor publică documentația, un atacator scanează. Diferența dintre un secret și o obscuritate este că secretul (cheia, parola) se poate schimba când este compromis; obscuritatea (modul în care funcționează sistemul) nu.

Tehnicile din această carte respectă principiul lui Kerckhoffs: toate sunt publice, descrise în detaliu, cunoscute de orice atacator — și funcționează oricum, pentru că securitatea lor stă în ceea ce atacatorul nu poate obține (cuvântul convenit față în față, a doua cheie, copia deconectată), nu în ceea ce nu știe.

Mitul 4: „Software-ul vechi este mai sigur, pentru că nu-l atacă nimeni”

Expertul finlandez Mikko Hyppönen a folosit ani de zile un program de e-mail din anii '90, pe motiv că nimeni nu mai scrie malware pentru el. Ideea — numită uneori „securitate prin antichitate” — are un sâmbure adevărat: atacatorii optimizează pentru țintele frecvente, iar un sistem rar este, statistic, mai puțin vizat.

Dar sâmburele este mic. Software-ul vechi nu mai primește corecții de securitate, iar vulnerabilitățile lui sunt publice, documentate și exploatabile cu instrumente gratuite. Dacă un atacator ajunge, din orice motiv, în fața lui, nu are nevoie de o campanie dedicată — are nevoie de cinci minute. Cele mai costisitoare incidente din sectorul medical și industrial din ultimul deceniu au implicat sisteme vechi, neactualizabile, lăsate în rețea pentru că „merg”. Atacul WannaCry din 2017 a paralizat spitale britanice tocmai pentru că rulau sisteme vechi, pentru care corecția exista de două luni.

Vechimea protejează doar un sistem care este și izolat (fișa 8). Un sistem vechi și conectat nu este obscur; este o ușă deschisă pe care nu o mai poate închide nimeni.

Mitul 5: „Dacă totul cade, trecem pe hârtie și ne descurcăm”

În 2018, districtul Matanuska-Susitna din Alaska a fost lovit de un atac care i-a scos din funcțiune toate sistemele. Funcționarii au trecut la mașini de scris și la chitanțe scrise de mână, iar administrația a continuat să funcționeze. Povestea a devenit celebră ca dovadă că „hârtia merge întotdeauna”.

A mers, cu un cost enorm, timp de săptămâni, într-o organizație care încă avea angajați care știau cum se lucra pe hârtie. Norsk Hydro (fișa 3) a supraviețuit în același fel, pentru că muncitorii mai vechi știau să opereze liniile manual. Peste zece ani, acei oameni nu vor mai fi acolo. O procedură manuală de rezervă este utilă doar dacă există, este scrisă, este exersată și dacă cineva o mai știe. Altfel, „trecem pe hârtie” este o frază, nu un plan.

Hârtia are, de altfel, propriile încălcări de securitate: dosare uitate în tren, arhive inundate, documente aruncate la gunoi fără distrugere, registre fotografiate cu

telefonul. Autoritățile de protecția datelor sancționează de ani de zile breșe în care niciun calculator nu a fost implicat.

Hârtia este o componentă a continuității, nu continuitatea însăși. Runbook-ul pe hârtie din fișa 3 funcționează pentru că este o verigă *proiectată* într-un lanț care rămâne, în rest, digital — nu pentru că hârtia ar fi, în sine, sigură.

Ce rămâne după mituri

Niciuna dintre cele douăsprezece tehnici din această carte nu funcționează pentru că este veche. Funcționează pentru că rezolvă o problemă structurală — încredere, separare, integritate, redundanță, detecție — într-un mod care nu depinde de tehnologia atacată. Vechimea este dovada că au fost testate, nu motivul pentru care merg. Iar testul final al oricăreia dintre ele nu este anul în care a fost inventată, ci secțiunea „Unde eșuează” din fișa ei.

Tabel de corelare: tehnici și obligații legale

Tabelul de mai jos arată la ce obligații contribuie fiecare tehnică, pentru a ușura documentarea măsurilor în registrul de securitate (art. 30 și 32 GDPR), în evaluarea riscurilor cerută entităților NIS2 sau în Declarația de aplicabilitate ISO/IEC 27001. Este un instrument de sprijin, nu o demonstrație de conformitate: o măsură corelată cu un articol dovedește că ați tratat un risc, nu că ați îndeplinit articolul. În ISO/IEC 27001, controalele se selectează și se justifică în procesul de tratare a riscurilor, iar GDPR și NIS2 cer măsuri adecvate riscului concret al organizației, nu o listă fixă. Referințele la NIS2 sunt la articolele Directivei (UE) 2022/2555; în România, transpunerea este OUG nr. 155/2024, aprobată cu modificări prin Legea nr. 124/2025, care preia aceleași măsuri cu numerotare proprie.

Nr.	Tehnica	GDPR	Directiva NIS2 (art. 21 alin. 2, cu excepțiile notate)	ISO/IEC 27001:2022, Anexa A
1	Parola de recunoaștere	art. 32	lit. (i) – control al accesului, resurse umane (nu ține locul MFA de la lit. j)	A.5.17, A.6.3, A.5.3
2	Regula celor doi	art. 25; art. 32 alin. (1) lit. (b)	lit. (i) – control al accesului (nu ține locul MFA de la lit. j)	A.5.3, A.8.2
3	Runbook-ul pe hârtie	art. 33 (evaluarea riscului, notificare), art. 33 alin. (5), art. 34	lit. (b) – gestionarea incidentelor; lit. (c) – continuitate și gestionarea crizelor; art. 23 – notificare	A.5.24–A.5.28, A.5.29–A.5.30
4	Sigiliul	art. 32 alin. (1) lit. (a) și (c)	lit. (h) – criptografie și gestionarea cheilor	A.8.24, A.5.17, A.7.10
5	Copia de la mănăstire	art. 32 alin. (1) lit. (c) și (d)	lit. (c) – copii de rezervă și recuperare în caz de dezastru	A.8.13, A.5.30
6	Compartimentarea	art. 5 alin. (1) lit. (c); art. 25; art. 32	lit. (i) – control al accesului, gestionarea activelor	A.5.15, A.5.18, A.8.3, A.8.22
7	Chirograful	art. 5 alin. (1) lit. (f); art. 32 alin. (1) lit. (b)	lit. (d) – lanț de aprovizionare; lit. (e) – achiziție, dezvoltare, întreținere	A.8.24, A.5.19–A.5.21, A.8.32, A.8.15
8	Mesagerul și spațiul gol	art. 32; art. 9 (date sensibile)	lit. (e); lit. (i)	A.8.22, A.7.10, A.8.12, A.8.31
9	Blocul de unică folosință	art. 32 alin. (1) lit. (a); art. 34 alin. (3) lit. (a)	lit. (h) – criptografie și criptare	A.8.24
10	Momeala	art. 33 (luarea la cunoștință); art. 32 alin. (1) lit. (d)	lit. (b) – detectarea incidentelor; art. 23	A.8.16, A.5.24–A.5.26
11	Codul de constrângere	art. 32	art. 21 alin. (1) – mediul fizic; lit. (i) – securitatea resurselor umane	A.7.1–A.7.4, A.6.3, A.6.8
12	Jurnalul santinelei	art. 5 alin. (2); art. 33 alin. (3) și (5)	lit. (b); lit. (f) – evaluarea eficacității măsurilor	A.8.15, A.8.16, A.8.17

Cum se citește tabelul invers

Tabelul poate fi folosit și pornind de la obligație, pentru a răspunde întrebării „ce măsură concretă pot documenta pentru această literă?”:

- **NIS2 lit. (b), gestionarea incidentelor:** runbook-ul pe hârtie (3), momeala (10), jurnalul santinelei (12).
- **NIS2 lit. (c), continuitate și copii de rezervă:** runbook-ul pe hârtie (3), copia de la mănăstire (5).
- **NIS2 lit. (d)–(e), lanț de aprovizionare și sisteme:** chirograful (7), mesagerul și spațiul gol (8).
- **NIS2 lit. (h), criptografie:** sigiliul (4), blocul de unică folosință (9).
- **NIS2 lit. (i), acces și resurse umane:** parola de recunoaștere (1), regula celor doi (2), compartimentarea (6), codul de constrângere (11).
- **NIS2 lit. (j), autentificare multifactor:** nicio tehnică din carte nu o acoperă singură; MFA pe conturi este o măsură tehnică distinctă, pe care fișele 1 și 2 o completează, nu o înlocuiesc.
- **GDPR art. 32 alin. (1) lit. (a), criptare:** sigiliul (4), blocul de unică folosință (9).
- **GDPR art. 32 alin. (1) lit. (b), integritate:** regula celor doi (2), chirograful (7).
- **GDPR art. 32 alin. (1) lit. (c), restabilirea disponibilității:** copia de la mănăstire (5), sigiliul (4).
- **GDPR art. 33, notificarea încălcărilor:** runbook-ul pe hârtie (3), momeala (10), jurnalul santinelei (12).

Costul direct al implementării celor douăsprezece tehnici, pentru o firmă de 20 de oameni, este mic — pungi sigilate, două discuri externe, eventual un laptop dedicat și câteva abonamente —, iar costul real este timpul oamenilor, de ordinul câtorva zile de lucru în prima lună și al câtorva ore pe lună după aceea; planul de acțiune le detaliază orientativ. Ele sunt măsuri accesibile care pot reduce semnificativ unele dintre riscurile cele mai frecvente, iar implementarea și documentarea lor sunt un punct de plecare onest pentru conformitate. Nu sunt un substitut pentru evaluarea riscurilor, pentru verificarea periodică a eficacității măsurilor și pentru ansamblul obligațiilor care se aplică organizației voastre.

Bibliografie adnotată

Sursele de mai jos sunt cele pe care se sprijină fișele. Sunt grupate pe tipuri, cu o frază despre ce aduce fiecare, pentru cititorul care vrea să meargă mai departe.

Surse antice și medievale

- **Polibiu**, *Istorii*, cartea VI (cap. 34–37). Descrierea taberei romane: parola zilnică (*tessera*), rondul de noapte, tăblițele santinelelor și pedepsele. Cea mai veche descriere tehnică a unui sistem de autentificare și de jurnalizare. Disponibil în traduceri moderne și online.
- **Biblia**, *Cartea Judecătorilor*, 12, 5–6. Episodul „șibolet” — autentificarea prin ceea ce impostorul nu poate imita.
- **Herodot**, *Istorii*, cartea V (cap. 52–54) pentru Drumul Regal și cartea VIII (cap. 98) pentru sistemul de curieri persan.
- **Cassiodor**, *Institutiones divinarum et saecularium litterarum* (c. 540–560). Manualul mănăstirii Vivarium: de ce și cum se copiază cărțile.
- **Pliniu cel Bătrân**, *Naturalis Historia*, cartea XXXIII. Despre inelele cu sigiliu și răspândirea lor.

Istorie și istoria tehnicii

- **David Kahn**, *The Codebreakers* (ed. revizuită, Scribner, 1996). Istoria de referință a criptografiei, de la antichitate la computer; sursa pentru Vernam, Mauborgne și contextul blocului de unică folosință.
- **Simon Singh**, *Cartea codurilor* (Humanitas, ed. rom.). Versiunea accesibilă a aceleiași istorii; capitolele despre Enigma și despre blocul de unică folosință.
- **Claude E. Shannon**, „Communication Theory of Secrecy Systems”, *Bell System Technical Journal*, 1949. Demonstrația secretului perfect.
- **Auguste Kerckhoffs**, „La cryptographie militaire”, *Journal des sciences militaires*, 1883. Principiul care îi poartă numele.
- **John Earl Haynes, Harvey Klehr**, *Venona: Decoding Soviet Espionage in America* (Yale University Press, 1999). Reutilizarea blocurilor și consecințele ei.
- **M.R.D. Foot**, *SOE in France* (HMSO, 1966; reeditări) și **Leo Marks**, *Between Silk and Cyanide* (HarperCollins, 1998). Verificările de securitate ale operatorilor radio, structura celulelor și, la Marks, autopsia sinceră a eșecului din Olanda (Englandspiel).
- **Richard Rhodes**, *The Making of the Atomic Bomb* (Simon & Schuster, 1986). Compartimentarea Proiectului Manhattan și cazul Fuchs.
- **Atul Gawande**, *The Checklist Manifesto* (Metropolitan Books, 2009). Accidentul Model 299 din 1935 și nașterea listei de verificare.

- **Denise Schmandt-Besserat**, *How Writing Came About* (University of Texas Press, 1996). *Bullae*, jetoanele și sigiliile-cilindru din Mesopotamia.
- **The National Archives (Regatul Unit)**, ghidurile de cercetare privind actele medievale (*deeds*, *indentures*) și colecția de *tally sticks* ale Trezoreriei. Descrierea documentelor tăiate și a bețelor de răboj, cu exemplare digitizate.
- **NSA**, *Learning from the Enemy: The GUNMAN Project* (Center for Cryptologic History, 2007, desecretizat). Mașinile de scris IBM Selectric din ambasada de la Moscova.
- **Jeremiah Denton**, *When Hell Was in Session* (1976). Mărturia prizonierului care a clipit „torture" în Morse.

Securitate informatică

- **Clifford Stoll**, *The Cuckoo's Egg* (Doubleday, 1989). Prima descriere a unui honeypot și a urmăririi unui intrus; se citește ca un roman.
- **Ben McCarty**, *Cyberjutsu: Cybersecurity for the Modern Ninja* (No Starch Press, 2021). Cea mai apropiată lucrare ca intenție de această carte: tehnici din manualele ninja aplicate la securitatea rețelelor.
- **Bruce Schneier**, *Secrets and Lies* (Wiley, 2000) și blogul *Schneier on Security*, eticheta „history of security". Sursa cea mai consecventă de gândire despre securitate ca problemă de oameni, nu de tehnologie.
- **Kim Zetter**, *Countdown to Zero Day* (Crown, 2014). Stuxnet și traversarea spațiului gol de la Natanz.
- **Andy Greenberg**, *Sandworm* (Doubleday, 2019). NotPetya, Maersk și controlerul de domeniu din Ghana.
- **Peter Krogh**, *The DAM Book* (O'Reilly, 2005). Formularea originală a regulii 3-2-1 pentru copiile de rezervă.
- **ENISA**, *Threat Landscape* (ediții anuale). Tendințele amenințărilor la nivel european; sursa pentru frecvența fraudelor BEC și a ransomware-ului.

Cazuri recente citate

- Ferrari, iulie 2024 — relatarea originală Bloomberg (Daniele Lepido) și analiza *MIT Sloan Management Review*, „How Ferrari Hit the Brakes on a Deepfake CEO".
- Arup, Hong Kong, ianuarie 2024 — relatările *Financial Times* și *CNN* despre transferul de 200 de milioane HKD obținut prin apel video cu deepfake-uri.
- SolarWinds, decembrie 2020 — raportul FireEye/Mandiant și analizele CISA.
- Norsk Hydro, martie 2019 — comunicările publice ale companiei, remarcabile prin transparență.
- Tesla, Nevada, august 2020 — actul de acuzare al Departamentului de Justiție al SUA în cazul Kriuchkov.

- Matanuska-Susitna, Alaska, iulie 2018 — relatarea *Washington Post* și raportul districtului.
- WannaCry, mai 2017 — raportul National Audit Office (Regatul Unit) despre impactul asupra NHS.

Cadrul legal

- **Regulamentul (UE) 2016/679 (GDPR)**, în special art. 5, 25, 32, 33, 34.
- **Directiva (UE) 2022/2555 (NIS2)**, în special art. 21 și 23.
- **OUG nr. 155/2024** privind cadrul de securitate cibernetică (transpunerea NIS2 în România), aprobată cu modificări și completări prin **Legea nr. 124/2025**, și ordinele DNSC de aplicare.
- **Legea nr. 123/2026**, care protejează cercetarea de securitate de bună-credință (raportarea responsabilă a vulnerabilităților) și întărește cooperarea DNSC cu autoritățile competente.
- **Regulamentul (UE) nr. 910/2014 (eIDAS)**, pentru semnătura electronică.
- **ISO/IEC 27001:2022** și **ISO/IEC 27002:2022**, pentru controalele din Anexa A citate în fișe.
- **Convenția de la Viena privind relațiile diplomatice (1961)**, art. 27, pentru inviolabilitatea valizei diplomatice.

Despre autor

Dan Gurghian este inginer în automatică și informatică industrială, cu peste douăzeci de ani de activitate în IT, dintre care peste cincisprezece în administrarea infrastructurilor de rețea și servere și în securitatea sistemelor informatice. Este director IT (CTO) al Amplusnet S.R.L. din Târgu Mureș, companie certificată ISO/IEC 27001 și ISO 9001, unde a proiectat și administrat, între 2010 și 2020, infrastructura serviciului internațional de VPN ibVPN — peste 250 de servere în peste 80 de țări —, a implementat și conduce Sistemul de Management al Securității Informației și coordonează serviciile de conformitate GDPR, NIS2 și securitate cibernetică oferite clienților sub marca GDPRComplet: responsabil cu protecția datelor externalizat pentru peste 200 de organizații din sănătate, industrie, retail, servicii financiare, administrație publică și educație, responsabil NIS2 pentru entități esențiale și importante, evaluări și audituri de securitate, sesiuni de instruire pentru angajați și management.

Este absolvent al programelor Directoratului Național de Securitate Cibernetică pentru auditori de securitate cibernetică (2023) și responsabili NIS (2024), ISO/IEC 27001 Lead Auditor, CompTIA Cybersecurity Analyst (CySA+) și analist de informații privind amenințările cibernetice (arcX), cu certificări Microsoft în administrarea și securitatea rețelelor Windows Server încă din 2002–2005. Și-a început cariera ca programator C++ la Infopulse, dezvoltând aplicații de securitate a rețelelor, inclusiv un sistem SIEM.

Această carte s-a născut din practica zilnică de consultanță și audit: din observația repetată că măsurile care previn cel mai des pagubele la clienți nu sunt cele mai scumpe, ci cele mai vechi.

Fișele din această carte, împreună cu altele noi, sunt publicate și actualizate la **gurghian.ro**.

Securitate veche pentru amenințări noi. Tehnici dinaintea internetului care încă funcționează
© Dan Gurghian, 2026. Prima ediție electronică.

Această lucrare poate fi distribuită gratuit, în forma ei integrală și nemodificată, cu menționarea autorului. Reproducerea parțială, în orice scop, se face cu citarea sursei.

Informațiile din această carte au caracter general și nu constituie consultanță juridică sau de securitate pentru o situație concretă. Referințele legale sunt la actele în vigoare la data publicării.