



BULETIN DE SECURITATE NIS2

Nr. 3 • Septembrie 2026

Stick-ul USB:

cel mai mic dispozitiv, unul dintre cele mai mari riscuri — plus fișierele din surse necunoscute

Material informativ pentru personalul instituției

Elaborat de DAF Consulting & Management SRL – responsabil NIS2 / CISO extern

De ce primiți acest material

Filtrele de e-mail și firewall-ul apără instituția dinspre internet. Stick-ul USB și fișierul descărcat intră pe ușa din spate — direct în calculatorul dumneavoastră.

1 stick

Un singur stick infectat, conectat de un singur angajat, poate opri sistemele unei instituții întregi. Unele dintre cele mai mari atacuri din istorie exact așa au început.



Obligație legală NIS2

Controlul suporturilor amovibile (stick-uri, harduri externe, carduri) face parte din măsurile de securitate impuse instituției.



USB-ul ocolește apărarea

Ce intră pe USB nu trece prin filtrele de e-mail și de internet ale instituției. Singurul filtru rămas sunteți dumneavoastră.



Datele ies la fel de ușor cum intră virușii

Un stick pierdut cu date de pacienți este o breșă de securitate — cu aceleași obligații de raportare ca orice alt incident.

Cum devine un stick o armă

Patru situații banale — toate folosite în atacuri reale asupra instituțiilor:



Stick-ul „găsit”

În parcare, pe hol, la recepție. Atacatorii le lasă intenționat — curiozitatea („al cui o fi?”) face restul.



Stick-ul de acasă

Folosit și pe calculatorul personal, și la serviciu. Ce a prins acasă (jocuri, descărcări) aduce la serviciu.



Cadoul promoțional

Stick-uri primite la conferințe, târguri sau de la vizitatori. Proveniență necunoscută = conținut necunoscut.



Fișierul descărcat

Programe „gratuite”, jocuri, „crack”-uri instalate pe cont propriu — una dintre cele mai directe căi de infectare.

Nu doar stick-urile: fișierele-capcană

Aceleași reguli de prudență se aplică fișierelor, indiferent cum ajung la dumneavoastră:



„Enable Content” în documente Office

Un document care vă cere să „activați conținutul” / macrocomenzile poate rula cod periculos. Dacă nu ați cerut documentul și nu-i cunoașteți sursa — nu apăsați butonul galben.



Arhivele cu parolă primite pe e-mail

Parola trimisă în același mesaj nu e „securitate” — e metoda prin care atacatorii ascund conținutul de antivirus. Tratați-le cu maximă suspiciune.



Extensiile înșelătoare

„Factura.pdf.exe”, „Rezultate.docx.js” — fișiere executabile deghizate în documente. Dacă extensia finală nu e cea așteptată, nu deschideți.



Programele instalate pe cont propriu

Orice program nou pe calculatorul de serviciu se instalează doar de către sau cu acordul IT. Inclusiv „utilitarele mici și gratuite” — mai ales ele.

6 reguli pentru suporturi și fișiere

Valabile pentru stick-uri USB, harduri externe, carduri de memorie și orice fișier primit sau descărcat:



Necunoscut = neconectat

Stick găsit, primit, „al nimănui”? Nu se conectează la niciun calculator al instituției. Se predă responsabilului IT.



Doar suporturi aprobate de IT

Pentru date de serviciu se folosesc exclusiv dispozitivele puse la dispoziție / aprobate de instituție, de preferat criptate.



Scanare înainte de folosire

Orice suport extern se scanează cu antivirusul înainte de a deschide fișiere de pe el. Durează un minut.



Datele de pacienți nu pleacă pe stick personal

Niciun export de date medicale sau de personal pe dispozitive proprii. Pentru transfer există canalele instituției.



Descărcări doar din surse oficiale

Programe și fișiere doar de pe site-urile oficiale și doar cu acordul IT — niciodată „crack”-uri sau arhive de pe forumuri.



Pierdut sau suspect? Raportați imediat

Stick pierdut, calculator care se comportă ciudat după o conectare — anunțați IT pe loc. Reacția rapidă limitează pagubele.

Ați găsit un stick? L-ați pierdut pe al instituției?



Ați găsit un stick

- Nu îl conectați — nici „doar ca să vedeți al cui e”. Exact pe această curiozitate mizează atacatorii.
- Predați-l responsabilului IT, care îl poate verifica în siguranță.
- Aceeași regulă pentru harduri externe, carduri de memorie sau alte dispozitive „uite”.



Ați pierdut un stick

- Anunțați imediat responsabilul IT — chiar dacă „probabil e pe undeva prin birou”.
- Notați ce conținea: date de pacienți? de personal? documente interne?
- Dacă avea date personale, poate fi o breșă cu obligații de raportare — evaluarea se face imediat, nu „când apare”.

Raportarea unui stick pierdut nu vă pune într-o lumină proastă — ascunderea lui, da.

Alternativa sigură: canalele instituției

De cele mai multe ori, stick-ul nici nu e necesar — transferul se poate face pe căi controlate și trasabile:



Rețeaua internă

Directoarele partajate (share-uri) ale instituției: fișierul rămâne în interiorul rețelei, cu drepturi de acces controlate.



Platformele aprobate

Sistemele informatice ale instituției și soluțiile de transfer puse la dispoziție de IT — inclusiv pentru fișiere mari.



Când USB-ul e totuși necesar

Doar dispozitivul aprobat de IT, de preferat criptat, folosit exclusiv pentru serviciu — și șters după utilizare.

Dacă un canal de care aveți nevoie lipsește, semnalați-i responsabilului IT nevoia — soluția corectă se construiește, nu se improvizează cu stick-uri personale.

Pe scurt: așa NU / așa DA

Așa NU

- Nu conectați stick-uri găsite, primite sau cu proveniență necunoscută
- Nu folosiți același stick și acasă, și la serviciu
- Nu copiați date de pacienți sau de personal pe dispozitive personale
- Nu instalați programe pe cont propriu și nu activați macrocomenzi la cerere
- Nu tratați pierderea unui stick ca pe un fleac — poate fi o breșă

Așa DA

- Predați IT-ului orice dispozitiv găsit, fără să-l conectați
- Folosiți doar suporturi aprobate de instituție, scanate înainte de utilizare
- Preferați canalele interne (share-uri, platforme) în locul stick-urilor
- Descărcați doar din surse oficiale, cu acordul IT
- Raportați imediat pierderea unui suport sau orice comportament ciudat al calculatorului

Regula de aur

• NU CONECTA • NU DESCĂRCA • RAPORTEAZĂ



1. NU CONECTA

Niciun dispozitiv necunoscut, găsit sau personal nu se conectează la calculatoarele instituției. Necunoscut înseamnă periculos — până la verificarea făcută de IT.



2. NU DESCĂRCA

Fără programe instalate pe cont propriu, fără fișiere din surse dubioase, fără „Enable Content” la documente neașteptate. Când aveți nevoie de ceva — cereți IT-ului.



3. RAPORTEAZĂ

Stick pierdut, dispozitiv găsit, calculator care se comportă ciudat — anunțați imediat responsabilul IT. Primele minute fac diferența între un fișier infectat și o instituție blocată.



Rețineți esențialul

Filtrele instituției nu văd ce intră pe USB. Acolo, singurul filtru sunteți dumneavoastră.

Un dispozitiv necunoscut rămâne neconectat, un program nou trece pe la IT, iar un stick pierdut se raportează în aceeași zi — nu „când o fi”. Prudența de câteva secunde protejează întreaga instituție.



Materialul face parte din programul lunar de informare și conștientizare NIS2 derulat de DAF Consulting & Management SRL pentru instituțiile pe care le asistăm în calitate de responsabil NIS2 / CISO extern.

Ediția următoare (octombrie 2026): Ransomware — cum îl recunoașteți și de ce contează primele minute.