Buju Stanciu & Asociații

Legal by Design

legea integrată în însăși cultura organizației

Buju Stanciu & Asociații

Despre prezentator

Alin Nichifor

Partener, Buju Stanciu & Asociații

Dreptul afacerilor și al tehnologiilor emergente

Lucrez la intersecția dintre lege, tehnologie și oameni.

Domenii în care inovația și riscul se întâlnesc.

Transform incertitudinea normelor juridice în încredere și structură.

Traduc complexitatea juridică în soluții.

Context actual: Amenințarea cibernetică în România

Creșterea atacurilor

Securitatea digitală devine o responsabilitate de management, nu doar o problemă tehnică. DNSC a gestionat **101 atacuri ransomware** în 2024, inclusiv incidente cu impact în sănătate și energie.

Rolul funcției juridice

Funcția juridică trebuie să traducă cerințele legale de cybersecurity în acțiuni concrete, protejând organizația de riscuri legale și reputaționale.

Directiva NIS2 – Schimbare de Paradigmă

Extindere

Mai multe sectoare sub obligație: esențiale și importante. De la energie și transporturi până la producție și alimentar.

Obligații cheie

Măsuri riguroase de securitate, evaluări de risc periodice, raportare incidente în 24-72h, înregistrare obligatorie.

Sancțiuni crescute

Până la **10 milioane EUR** sau **2% din cifra globală** pentru entități esențiale. Până la **7 milioane EUR** sau **1,4% din cifra globală** pentru entități importante.

Atenție: NIS2 introduce conceptul de responsabilitate personală a conducerii - membrii funcțiilor de conducere pot fi considerați responsabili pentru neglijență în supravegherea riscurilor cibernetice la nivelul entității și pot fi sancționați individual prin interdicția temporară a exercitării funcției pe care o ocupă

Identificarea și Clasificarea entităților

Entități esențiale

- Energie, transport, sănătate
- Apă, infrastructură digitală
- Administrație publică
- Cercetare

Entități importante

- Servicii digitale
- Producție alimentară
- Chimicale, waste management
- Chiar și întreprinderile mici pot intra sub incidență

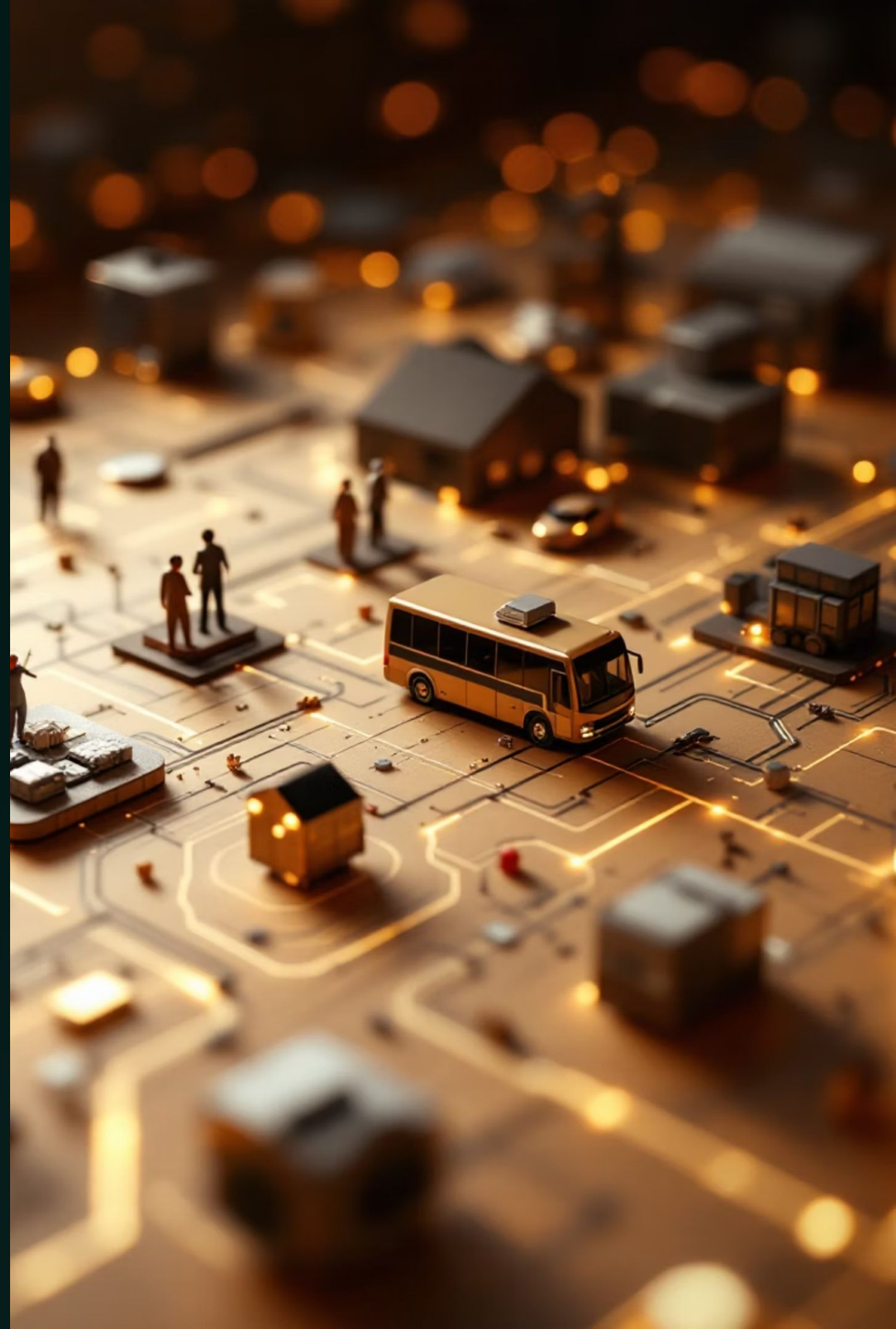
DNSC – platforma NIS2@RO

Instrument de autoevaluare a conformității.

Pentru societățile *borderline*, încadrarea rămâne neclară

Notificarea către DNSC este recomandată pentru clarificare

Un proces nou, birocratic, care a generat confuzie și aglomerare.



Autoevaluare NIS2 vs. Audit ISO 27001 – Efort dublu sau sinergie?

Obligație legală

entitățile esențiale/importante trebuie să facă **autoevaluare anuală** a nivelului de maturitate a securității cibernetice și să o raporteze la DNSC

Certificare ISO 27001

certificare valabilă **3 ani** (cu audituri de supraveghere anuale) - – **NU înlocuiește autoevaluarea NIS2** (obligație legală distinctă, cu format și cerințe specifice)

Provocare

evaluare dublă– un efort birocratic suplimentar și alocare de resurse extra pentru conformare (ISO și NIS2).

Recomandare

sinergie între ISO și NIS2 - – folosiți auditul ISO ca bază tehnică, dar **realizați autoevaluarea în formatul cerut de DNSC,** cu aprobarea formală a managementului.

Buju Stanciu & Asociații

Obligații de raportare a incidentelor

01

Notificare inițială

Informare DNSC în **24 de ore** de la detectarea incidentului major

02

Raport detaliat

Transmitere raport complet în **72 de ore**

03

Raport final

Document final în termen de **o lună**

04

Informare clienți

Notificare directă utilizatori afectați fără întârziere

Fereastra de raportare s-a scurtat semnificativ. Scopul este ca autoritățile să afle foarte rapid și să poată coordona răspunsul la incidente.

„Dublă Lovitură”: GDPR + NIS2

Un singur atac

două legi. două autorități.
o cursă contracronometru

✔️ sisteme blocate → notificare **DNSC** (NIS2) în **24h**

✔️ date personale compromise → notificare ANSPDCP (GDPR) în **72h**

Obligații paralele,

nu alternative

→ formulare diferite

→ praguri de notificare diferite

→ riscuri legale + reputaționale cumulative

Provocare reală

echipa de răspuns trebuie să lucreze sincronizat:

- să evalueze rapid impactul serviciului vs. riscul pentru persoană
- să redacteze două notificări clare și separate
- să comunice cu două autorități în paralel

"DNSC nu poate sancționa o entitate pentru un incident aflat în investigația ANSPDCP – un mecanism de echilibru juridic"

Externalizarea nu externalizează responsabilitatea

Contracte de cloud sau MSSP?

organizația rămâne 100% responsabilă

Control strict al furnizorilor terți

due diligence riguros, clauze de securitate în contracte, audituri periodice la parteneri, termene de notificare scurte

„Poți externaliza munca, dar nu și vina.”

în caz de incident, organizația ta va fi răspunzătoare.

Recomandare

Tratați riscurile furnizorilor ca parte integrantă din strategia de guvernanță cibernetică a firmei

Buju Stanciu & Asociații

Dilema Răscumpărării

Argumente PRO plată

- Soluție rapidă – reluare activitate
- Paguba directă: sumă cerută
- Downtime costă mai mult

Argumente CONTRA plată

- Nicio garanție de recuperare
- Dublă extorsiune – pot publica datele oricum
- Posibil ilegal – finanțare terorism
- Alimentăm cercul vicios
- Plata nu “șterge” obligațiile de notificare

Decideți politica față de ransomware din timp (și implicați juridicul în decizie), nu în toiul crizei când sunteți sub presiune.

DORA – Reziliența Digitală în Sectorul Financiar

01

Management robust al riscurilor

Inventar complet al sistemelor, evaluări continue, politici de securitate la nivel de grup

02

Teste periodice de reziliență

Penetration testing, simulări de atac - "crash-test" al infrastructurii digitale

03

Raportări rapide și uniforme

Incidente majore raportate rapid, cadru unificat de clasificare

04

Supraveghere furnizori critici

Cloud și provideri IT critici sub supraveghere directă a autorităților

Digital Operational Resilience Act - model de reglementare strictă pentru sectorul financiar (bănci, asigurări, fonduri) care ar putea fi extins în alte industrii.

Recomandări pentru conformare

1 Verificați încadrarea legală

Determinați statutul (esențial/important) și înregistrați-vă la DNSC pe platforma NIS2@RO.

2 Efectuați analiza gap

Identificați neconformități și construiți roadmap cu responsabilități, bugete și termene clare.

3 Stabiliți guvernanța

Numiți CISO, creați comitet de securitate, includeți riscul cibernetic în registrul riscurilor la nivel de managementi.

4 Investiți în formare

Training periodic pentru management și angajați. Simulări de phishing și exerciții table-top.

5 Formalizați cyber playbook

Plan de răspuns la incidente cu proceduri clare de escaladare, notificare și recuperare.

6 Gestionați lanțul de aprovizionare

Clauze de securitate în contracte, evaluări periodice ale furnizorilor critici, audituri externe.

Securitatea cibernetică = prioritate strategică

Leadership

Nu doar o problemă tehnică - temă de guvernanță și supraviețuire a afacerii

Conformare Legală

Nu opțională - parte din responsabilitatea de business și due diligence

Investiție Strategică

În securitate = în încredere, reputație și viitorul companiei

> "Cybersecurity is a Team Sport - echipa include acum și juriștii, și directorii din top management, nu doar echipa IT."

Întrebarea Finală

Ce veți face mâine, diferit de ieri?

Veți aștepta o criză sau veți acționa acum?

În joc nu sunt doar date sau sisteme, ci viitorul afacerii voastre.

Securitatea cibernetică nu mai e o alegere tehnică, ci o alegere strategică de supraviețuire.

Buju Stanciu & Asociații

Let’s write your next chapter together.

bsa.ro | office@bsa.ro

Str. Belgrad 10, Sector 1, București