Tema 2 Managementul riscului

1. REZILIENȚĂ CIBERNETICĂ STRATIFICATĂ

Nivel 1 - Detecție Amenințări

* Implementare Wazuh EDR
* Senzori avansați de monitorizare rețea IDS/IPS
* Corelarea evenimentelor de securitate
* Machine Learning pentru detecție anomalii
* Hărți dinamice de threat intelligence

Nivel 2 - Răspuns Incidente

* Echipă dedicată SOC (Security Operations Center)
* Protocoale automate de izolare
* Scenarii simulate de răspuns rapid
* Sistem de alertare ierarhizat
* Înregistrare și analiză forensică completă

Nivel 3 - Recuperare

* Sisteme backup distribuite geografic
* Redundanță infrastructură critică
* Planuri de continuitate business
* Teste periodice de recuperare dezastru

1. PROTECȚIE DATE PERSONALIZATĂ

Strategie GDPR Avansată

* Hărți complete de flux date
* Mecanisme granulare de consimțământ
* Toolkit automat de minimizare date
* Proceduri stricte de ștergere date

Control Acces Multinivel

* Autentificare Zero Trust
* Principiul "least privilege"
* MFA adaptiv (behavioural authentication)
* Verificări continue de identitate
* Jurnale detaliate de access

1. MANAGEMENT STRATEGIC RISCURI

Metodologie Complexă

* Hartă de risc dinamică
* Scenarii simulate cuantificate
* Evaluări trimestriale detaliate
* Buget dedicat securității (min. 15% IT)

Tipuri Risc Acoperite

* Risc tehnic
* Risc operațional
* Risc reputațional
* Risc financiar
* Risc de conformitate

1. ARHITECTURĂ SECURITATE ADAPTABILĂ

Design Principii

* Microservicii securizate
* Criptare la nivel aplicație
* Monitorizare continuă comportament

Componente Cheie

* Gateway securitate next-gen
* Load balancers securizați
* Sisteme detecție/prevenție intruziuni
* Firewall-uri adaptative
* Filtrare trafic inteligentă

Recomandări Implementare:

1. Platformă integrată securitate
2. Program training continuu
3. Audit extern periodic
4. Implementare gradată

Costuri Estimate:

* Investiție inițială: 250.000 - 500.000 euro
* Mentenanță anuală: 15-20% din investiție
* Reducere potențială risc: 70-85%

Beneficii Strategice: ✓ Rezistență cibernetică crescută ✓ Încredere client consolidată ✓ Conformitate reglementări ✓ Flexibilitate tehnologică ✓ Avantaj competitional

Potențial Impact Financiar din Atac Cibernetic:

Cifra de afaceri eMag (2023): ~1.2 miliarde euro

Scenarii Posibile de Pierderi:

1. Atac Minor (24-48 ore downtime)

* Pierderi directe: 3-5% din vânzări zilnice
* Estimat: 1-2 milioane euro
* Costuri recuperare: 500.000 - 750.000 euro

1. Atac Mediu (3-7 zile)

* Pierderi directe: 7-12% din vânzări
* Estimat: 5-7 milioane euro
* Costuri recuperare: 1-1.5 milioane euro
* Pierdere potențială clienți: 15-20%

1. Atac Major (>1 săptămână)

* Pierderi directe: 15-25% din vânzări
* Estimat: 10-15 milioane euro
* Costuri recuperare: 2-3 milioane euro
* Pierdere potențială clienți: 30-40%
* Impact reputațional pe termen lung

Costuri Suplimentare:

* Investigații forensice
* Compensații clienți
* Penalități GDPR
* Refacere infrastructură
* Campanii de relansare încredere

Concluzie: Investiția în securitate (250.000-500.000 euro) reprezintă sub 5% din potențialele pierderi într-un scenariu de atac major.