Soluții IT
IMPLEMENTARE
GDPR

PHOENIX IT SOLUTIONS

Mihaela NEACȘU

Despre PHOENIX IT

- Tradiție de peste 12 ani în **domeniul consultanței IT&C**
- **Integrator de proiecte** ce cuprind mai multe tehnologii hardware și software, inclusiv soluții de securitate
- Datacenter Phoenix IT (respectă standard TIA 942, Tier 3)
- **Parteneriate cu lideri în tehnologie:**

Microsoft Partner
Gold OEM
Gold Software Asset Management
Silver Datacenter
Silver Volume Licensing
Silver Collaboration and Content
Silver Midmarket Solution Provider

intel Technology Provider

VERITAS Partner Force

ORACLE Gold Partner

VEEAM

FORTINET SILVER PARTNER

Bitdefender GOLD PARTNER

Symantec.

cisco

KASPERSKY lab

Extreme Customer-Driven Networking

Securitatea prelucrărilor de date

Art. 24
Responsabilitatea operatorului

Operatorul pune în aplicare

măsuri tehnice şi organizatorice adecvate

pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament.

Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.

Etapele realizării conformității – proiect de consultanță

Conformitate cu GDPR

Analiza culturii organizaționale în contextul GDPR

- Date și categorii de date personale prelucrate
- Contextul prelucrărilor
- Fluxuri operaționale de activități de prelucrare date
- Legislația existentă. Contracte. Împuterniciri.

Analiza măsurilor de securitate existente în context GDPR

Evaluare conformitate

Activități procedurabile necesare

- Stabilire responabilități organizatorice pe diverse arii
- Actualizări proceduri existente,crearea de proceduri noi
- Cereri de acces/ștergere/portabilitate
- Notificări
- Planuri de acțiune, evaluări periodice.

IMPLEMENTARE

Măsuri tehnice necesare pentru securitatea datelor

- Securitate infrastructură IT&C - actualizare
- Securitate fizică - actualizare
- Instruire personal.

Implementări Clienți

Selecție

- **Platformă instruire angajați – Secretariatul General al Guvernului**
  - actualizări asupra procedurilor interne, normelor și metodologiilor de aplicat
  - testarea angajaților direct în platformă
- **Consultanță IT Asset Management:**
  - MedLife
  - Spitalul Județean de Urgență Bacău
- **Securizare – Spitalul Județean de Urgență Bacău**
  - Intervenție depanarea rețelei în urma virusării cu ransomeware WannaCry
  - securizare rețea – firewall FortiGate
  - securizarea stațiilor de lucru și serverelor – Bitdefender GravityZone Enterprise

Implementări Clienți

Selecție

- **Securizare – Direcția Generală Asistență Socială și Protecția Copilului Sector 3**
- **securizarea 300 stații de lucru, serverelor și securizare email** – Bitdefender GravityZone Enterprise

- **Securizare 1600 stații de lucru si 200 servere fizice și virtuale** – Bitdefender GravityZone Enterprise – **Registrul Auto Roman**

- **Sistem integrat Registrul Agricol – Consiliul Județean Prahova, Consiliul Județean Bihor**
  - Securizare comunicații între UAT-uri din județ și CJ – VPN
  - Securizare rețele – firewall FortiGate
  - Securizare stații de lucru de la CJ și UAT-uri – Bitdefender/Symantec

Implementări
Clienți

Selecție

Workshop Soluții IT

Managementul riscurilor de Securitate și asigurarea conformității cu cerințele locale și internaționale, la nivelul întregii țări

Studiu de caz: Registrul Național de Medicină Legală, 42 de județe

Conformitatea cu GDPR

Identificarea și implementarea măsurilor necesare pentru a proteja prelucrările de date personale împotriva:

- prelucrării neautorizate sau **ilegale**;
- pierderii, a **distrugerii** sau a deteriorării accidentale.

Identificarea și implementarea măsurilor adecvate pentru:

- a asigura **confidenţialitatea**, **integritatea**, **disponibilitatea** şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare;
- a **restabili** disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- **instruirea** personalului operatorului de date;
- **testarea**, evaluarea şi aprecierea **periodice** ale eficacităţii măsurilor necesare pentru securitatea prelucrării.

Pentru a aduce în concret lucrurile pe care o instituție le poate face pentru a fi conformă cu regulamentul GDPR, norme/standarde:

Rolul integratorului Securitate din proiectare

(Security by design)

Activitati pe care o instituție trebuie sa le faca pentru a fi conformă cu regulamentul GDPR, norme/standarde:

- **Securizarea perimetrului fizic**
  - ✓ carduri de acces, acces pe bază de amprentă
  - ✓ monitorizare video a spațiilor unde se păstrează sau procesează datele
- **Securizarea fizică a echipamentelor hardware**
  - **Stații de lucru/laptopuri**:
    - ✓ cu modul de securitate TPM
    - ✓ cu funcționalitatea Windows BitLocker – securitate suplimentară prin PIN pentru prevenirea accesării datelor în cazul furtului sau pierderii accidentale a terminalului
    - ✓ Stick-uri (flash) de memorie criptate pe USB, cu parola

Servere:

- ✓ carcase speciale – montare cifru sau cheie sau lacăt
- ✓ cu protecție suplimentară fizică – dulap cu lacăt

In concret, lucrurile pe care o instituție le poate face pentru a fi conformă cu regulamentul GDPR, norme/ standarde:

Rolul integratorului Securitate din proiectare

(Security by design)

Phoenix Myway OfficePower EX

Complet administrabil de la distanță, independent de sistemul de operare și cu suport pentru o vastă suită de elemente de securitate, OfficePower EX este sistemul potrivit mediilor unde securitatea și eficiența sunt imperative.

DESTINAȚIE, UTILIZARE ȘI BENEFICII

Configurația de bază are suport deplin pentru tehnologiile Intel® vPro® și iAMT® 9.0. Sistemul este destinat mediilor unde administarea și securitatea centralizată sunt necesare.

Descriere:

Suportă procesoare Intel® Core® i5 și i7 cu tehnologiile Intel® vPro® și iAMT® - pe chipset Intel Q170;

Slot de securitate TPM 1.2;

Conform normelor europene privind electrosecuritatea, compatibilitatea electromagnetică și eficienţa energetică;

Carcasă SFF desktop-tower cu numeroase opțiuni de securizare fizică și surse cu eficienţă 80+ şi A-PFC;

Certificat Energy Star 6.1 și Microsoft WHQL pentru sistemele de operare Windows.

Rolul integratorului Securitate din proiectare

(Security by design)

Phoenix Myway eXpertServer 222-S

Server dual-procesor, format rack 2U și surse redundante.
Destinat companiilor cu nevoi mari de putere de procesare.

DESTINAȚIE, UTILIZARE ȘI BENEFICII
Soluția eXpertServer 222-S-2U este una dintre cele mai flexibile și scalabile. Este **alegerea perfectă pentru aplicații de tip baze de date sau soluții de virtualizare**.
Certificările Microsoft/VMware deținute recomandă această platformă ca pe una ideală pentru scenarii diverse de virtualizare.

Descriere:
Acceptă două procesoare Intel® Xeon® Scalable;
Max. 3 TB RAM DDR4 ECC REG, arhitectură Six-Channel;
PCIe Gen 3.0, modul expansiune I/O, eUSB, M.2;
8x3.5” bay hot-swap HW RAID 0, 1, 10, 5, 6 & backup battery, opțional SSD NVMe;
Format 2U rackmount, sursă 1300W 1+1 redundantă, certificare energetică 80 Plus Platinum;
Dual 10GbE RJ45 (opțional 10/25 GbE, Omni-Path 58/100 Gbps), tehnologie virtualizare;
Management IPMI 2.0, Remote Management inclus.

Rolul integratorului

Security by design

❖ Securizarea rețelei

❖ Firewall – Fortinet FortiGate

- ✓ Filtrarea traficului
- ✓ Blocarea accesului din intern la site-urile detectate ca având conținut periculos
- ✓ Segregrea rețelei pe departamente cu profile și drepturi de accesare diferite
- ✓ Mecanisme de prevenire a scurgerii de date după anumite cuvinte cheie stabilite
- ✓ Blocarea traficului de la IP-uri detectate și marcate în black list ca fiind periculoase
- ✓ Realizare tuneluri VPN între mai multe locații – clientul VPN este gratuit

❖ Securizarea email-ului

- ❖ FortiMail – antivirus și antispam pentru căsuțe de email pe orice server de email; scanare în atașamente

Rolul integratorului

Security by design

❖ Securizarea aplicațiilor Web - FortiWeb

- protejare contra vulnerabilitatile la nivel de cod din aplicatiile web;
- **protejare impotriva atacurilor hackerilor de tip SQL injection, de atacuri XSS (Cross-site Scripting)** si altele;
- protejarea preventiva impotriva defaimarii site-urilor web ale institutiei
- **conformare cu standardul PCI DSS (6.6) in folosirea cardurilor de credit si a datelor de sanatate (in cazul pacientilor, serviciilor medicale);**

❖ Analiză a traficului de rețea constantă în vederea prevenirii accesului neautorizat

- Loguri si alerte de securitate din FortiGate, FortiWeb, FortiSIEM
- Loguri si rapoarte agregate din FortiAnalyzer

Rolul integratorului

Security by design

Top User Sources By Sessions

#	User (or IP)	Source IP	Sessions
1	192.168.2	192.168.	17,478,741
2	192.168.2	192.168.	8,989,047
3	192.168.1	192.168.	2,166,312
4	192.168.1	192.168.	1,432,756
5	192.168.1	192.168.	1,166,436
6	192.168.1	192.168.	1,158,875
7	10.50.1.14	10.50.1.1	1,051,139
8	192.168.1	192.168.	1,047,334
9	192.168.1	192.168.	1,007,862
10	10.34.1.18	10.34.1.1	940,581
11	192.168.1	192.168.	932,421
12	192.168.1	192.168.	930,980
13	10.50.1.11	10.50.1.1	905,095
14	10.50.1.11	10.50.1.1	814,930
15	10.33.1.22	10.33.1.2	800,186
16	10.64.1.14	10.64.1.1	762,689
17	10.68.1.13	10.68.1.1	762,103
18	10.33.1.18	10.33.1.1	710,055
19	192.168.1	192.168.	706,099
20	10.37.1.16	10.37.1.16	678,451

Top Critical Threats Crossing The Network

#	Attack Name	Reference	Total Num
1	OpenSSL.Heartbleed.Attack	http://www.fortinet.com/ids/VID38315	102
2	Bash.Function.Definitions.Remote.Code.Execution	http://www.fortinet.com/ids/VID39294	42

Top High Threats Crossing The Network

#	Attack Name	Reference	Total Num
1	SSLv2.Openssl.Get.Shared.Ciphers.Overflow.Attempt	http://www.fortinet.com/ids/VID13227	1,075

Rolul integratorului

Security by design

Phoenix Security Appliance – dublă validare tehnologică hardware și software – Intel și Fortinet

Avantaje față de echipamentele/appliance-urile de securitate tradiționale:

• Funcționalitățile însumate ale mai multor echipamente, comprimate într-unul singur

• Flexibilitate și scalabilitate, conferite atât de configurabilitatea eXpertServer, cât și mașinile virtuale Fortinet;

• Funcționalitățile nu sunt legate de un anumit echipament fizic, licențele aplicațiilor virtuale Fortinet putând fi oricând migrate pe alte echipamente;

• Se pot oricând adăuga noi funcționalități pe același echipament, prin adăugarea de aplicații virtuale Fortinet și, eventual, upgrade-ul echipamentului eXpertServer;

• Backup și restaurare simplificate: restaurarea se poate face pe orice server de mașini virtuale.

Rolul integratorului

Security by design

Phoenix Security Appliance – dublă validare tehnologică hardware și software – Intel și Fortinet

Security Appliance 122-E3-1U

PREȚ DE LA 15.530$

eXpert SERVER

SPECIFICAȚII
1x Intel Xeon 4-core 3GHz, 16GB RAM ECC (max 64GB), 1.6TB SSD (max 1.9TB), 6x1Gbps RJ45, 1x PSU, remote management

Software instalat cu 1 an de suport inclus:
• Fortigate VM
• Fortianalyzer VM (1 GB/Day of Logs and 500 GB storage capacity)
• Fortimail

Ofertă specială pentru participanții la conferință:

- ❖ **15% discount pentru soluția integrată Phoenix Security Appliance**
- ❖ **Punere în funcțiune și configurare de bază incluse în prețul soluției**

IMPLEMENTARE

GDPR

Conformitate cu GDPR

Security by design

email

Acces informatic

Acces fizic

Trafic rețea

Aplicații

Stocare date

Prevenirea pierderii datelor, la transmitere din interior

IMPLEMENTARE

GDPR

Conformitate cu GDPR

Security by design

Categorie soluții	Articol regulament	Soluție
Auditul userilor, monitorizarea accesului și credențialelor	5,19,24,25, 32,33	Active Directory, Managementul identității
Backup și Arhivare	24,32,34	NetBackup, Enterprise Vault (arhivare fisiere, email si cautare in arhive)
Conformitate și retenția datelor	5,17,20,25, 32	Veritas Enterprise Vault (arhivare cu aplicare politici de retenție)
Criptare	32	Endpoint Encryption - Symantec
Gestionarea accesului la date	25	Active Directory, VPN, Security Group Policies
Monitorizarea evenimentelor din rețea, Gestionarea amenințărilor	5,24,25	SIEM - FortiSIEM
Gestionarea răspunsului la incidente	33	Cyber Security Services
Monitorizarea, localizarea și clasificarea datelor	5,9,12,18,20, 25,30	eDiscovery, Data Insight, Resiliency Platform - Veritas
Securitatea și prevenirea pierderii datelor	5,24,25,34	Data Loss Prevention (DLP) - Symantec

IMPLEMENTARE

GDPR

Rolul integratorului

Security by design

❖ Inventarierea:

- tuturor tipurilor de date cu caracter personal/special
- tuturor locațiilor fizice, aplicațiilor și echipamentelor hardware unde există date cu caracter personal/special, atât în scop de prelucrare, cât și de stocare sau arhivare
- tuturor tipurilor de formate de stocare a datelor cu caracter personal/ special
- Tuturor funcțiilor și rolurilor din instituție care intră în contact cu datele cu caracter personal/special

In funcție de aceste 4 inventare se pot stabili reguli de protecție și prevenire a scurgerilor de date sau de acces neautorizat de la caz la caz.

Soluția **Symantec Data Loss Prevention (DLP)**

Descoperă unde sunt stocate datele stabilite ca fiind confidențiale – indiferent dacă acestea se află pe un server sau pe echipamentele utilizatorilor
Monitorizează modul de manipulare al datelor, în rețea și în afara rețelei
Protejează împotriva furtului de date, inclusiv daca acestea sunt stocate in cloud sau pe device-uri mobile ale angajaților

IMPLEMENTARE

GDPR

Rolul integratorului

Security by design

Implicarea pacientului in actul medical – Casebond – Soluție de Patient Relationship and Case Management

- ✓ Preluarea consimantului informat al pacientului
- ✓ “Online check-in” pentru consultatii si internari
- ✓ Vizualizarea istoricului platilor si plata cu ajutorul CaseBond
- ✓ Programare pentru consultatii si internari
- ✓ Notificari (pentru programari, rezultate de laborator, etc.)
- ✓ Rezultate de laborator si imagistica
- ✓ Bilete de trimitere
- ✓ Vizualizarea istoricului medical
- ✓ Monitorizarea satisfactiei pacientului
- ✓ Mesagerie securizata
- ✓ Extinderea posibila pe orice proces care implica o interactiune cu pacientul
- ✓ Acces din browser sau de pe mobil/smartphone/tabletă

In viitor: autentificare pe baza de eID, cerinta obligatorie din 28 Septembrie 2018

IMPLEMENTARE

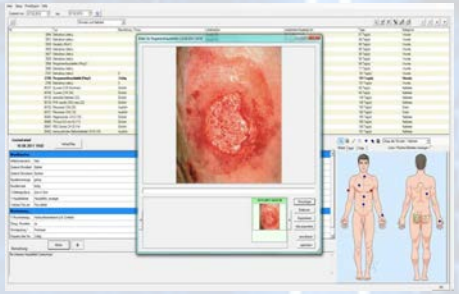
GDPR

Rolul integratorului

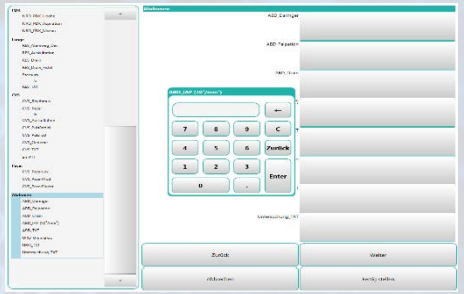
Security by design

QCare - Soluție pentru Terapie Intensivă

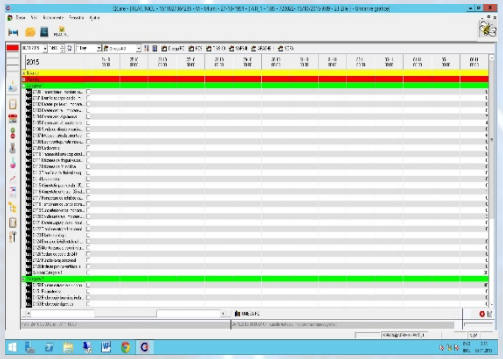
Vedere de Ansamblu



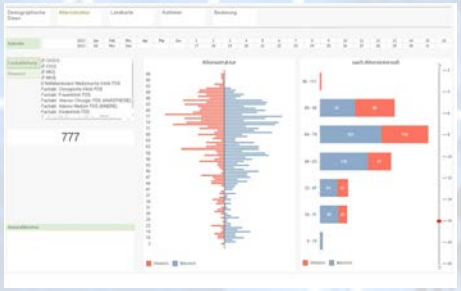
Modulul de Îngrijire Răni cu posibilitate de integrare PACS



Touch-screen



Scoruri (OmegaRO, GCS, TISS 10, SAPS II, SOFA, APACHE II, etc..)



Rapoarte

Diagrame date Clinice

Soluția Mobilă

IMPLEMENTARE

GDPR

Rolul integratorului

Security by design

“One-stop-shop” pentru soluții de creștere a securității și protecție a datelor personale/speciale/confidențiale:

- soluții **hardware**

- soluții de **virtualizare cu funcționalități de securitate la nivel de hypervisor și containere virtuale** pentru segregare și securitate inclusiv împotriva tentativelor de accesare neautorizată a aplicațiilor cu date sensibile din mașinile virtuale, de către administratorului serverului fizic

- soluții **software de backup, antivirus, protecție și prevenire**

- soluții de **baze de date cu funcționalități de securitate și auditare avansate**: Microsoft SQL Server, Oracle Database

- aplicație de interacțiune în mod securizat cu pacienții pe diverse cazuri

- aplicație de instruire la distanță a angajaților și testare

- consultanță, instruire și auditare – recomandări concrete de creștere a securității și conformității cu regulamentul și standardele de securitate a informației

IMPLEMENTARE

GDPR

Rolul integratorului

Security by design

“One-stop-shop” pentru soluții de creștere a securității și protecție a datelor personale/speciale/confidențiale:

- Soluțiile pot fi oferite în regim de **servicii, cu plată lunară**, “as a service” din Datacenterul Phoenix IT, locat într-o zonă nonseismică din România

- **Servicii de infrastructură IaaS**
  - **Servere virtuale securizate**
  - **Firewall**
  - **Monitorizare rețea**
  - **Backup**
  - **Disaster Recovery - spații de stocare scalabile și predefinite**

  Datele critice ale clientului sunt protejate în întregime în cazul:
  - dezastrelor naturale
  - defecțiunilor unor echipamente ale clientului
  - atacurilor cu viruși
  - erorilor umane
- **Servicii de SaaS (Software-as-a-Service)**
  - **aplicație eLearning**
  - **aplicație de Management al relației cu Pacienții**
- **Servicii de webhosting**
- **Servicii de colocare**

Mulțumim pentru atenție!

GENERAL DATA PROTECTION REGULATION

PHOENIX
IT SOLUTIONS

Implementări
Clienți

Selecție

Workshop Soluții IT

Managementul riscurilor de Securitate și asigurarea conformității cu cerințele locale și internaționale, la nivelul întregii țări

Studiu de caz: Registrul Național de Medicină Legală, 42 de județe

Workshop Solutii IT

Implementări Clienți

Selecție

Detalii organizatie Beneficiar:

- Institutul National de Medicina Legala Bucuresti
- 40 de Servicii Judetene de Medicina Legala din toata tara

Sistemul gestioneaza cazuri diverse, continand date avand caracter de informatie sensibila din perspectiva securitatii informatiei:

- Alcoolemii
- Emitere certificate medico-legale, ca urmare a situatiilor de violenta
- Teste de paternitate
- Autopsii
- Analize de laborator diverse

Numar utilizatori: 420 medici, asistenti, economisti, secretari

Workshop Solutii IT

Implementări Clienți

Selecție

Aplicatia de Management al Cazurilor Medico-Legale contine:

- Date avand caracter personal
- Date cu regim medical
- Documente emise oficial utilizate in diverse spete in Justitie

Provocarea in asigurarea securitatii datelor din sistem:

- Securizarea accesului in reteaua RNML si a traficului
- Securizarea aplicatiei web de management al cazurilor
- Securizarea conectarii utilizatorilor la aplicatie, fiind necesara asigurarea identitatii fizice a persoanelor care introduc si lucreaza pe cazuri

Workshop Solutii IT

Implementări Clienți

Selecție

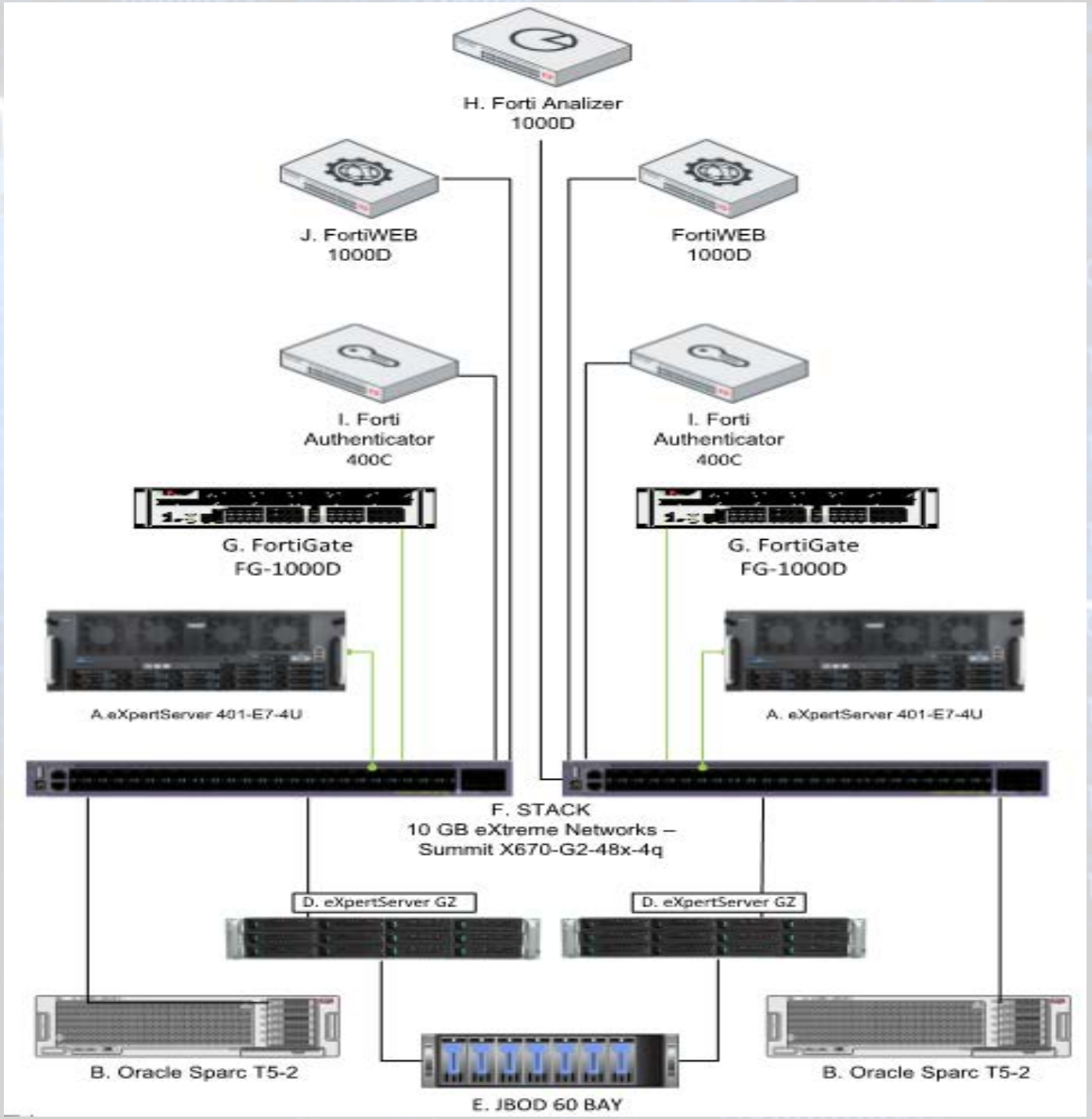
Solutia tehnica care asigura **securitatea by design**:

- Firewall: 2 x FortiGate 1000D
- Securizare aplicatie web: 2 x FortiWeb 1000D
- Acces utilizatori securizat – autentificare cu 2 factori:
  - conexiune VPN - FortiClient
  - user si parola – Active Directory - Microsoft Windows Server
  - 2 x FortiAuthenticator 400C
  - Forti Token (fizic- nominal) – generare parola de acces la nivelul fiecarui utilizator
- Analiza loguri Securitate: FortiAnalyzer 1000D

Workshop Solutii IT

Implementări Clienți

Selecție



Workshop Solutii IT

Provocări existente

Care este provocarea IT cu care vă confruntați in cadrul instituției?

- Securitate rețea
- Securitate echipamente de lucru
- Securitate servere
- Monitorizare echipamente
- Monitorizare rețea
- Capacitate de stocare
- Arhivarea datelor
- Regăsirea datelor
- Prevenirea pierderilor de date
- Necunoașterea în amănunt a parcului IT existent
- Lipsa unui punct de recuperare în caz de dezastru/ acces nedisponibil din cauze naturale sau incendiu
- Altele

Workshop Solutii IT

Conformitate GDPR

Vă mulțumesc!

Mihaela.neacsu@phoenix-it.ro

cerinte tehnice
libera circulatie
monitorizare
asumare
controlor
portabilitate
categorii
raspundere
procesator
ANSPDCP
rectificare
bresa de securitate
evidenta
prelucrare
stergere
cookie
identificabil
IP uri
electronic
transparenta
amenzi
justitie
GDPR
plangere
identificatori
proceduri
notificare
tert
securitate
parola
protectie
impact
DPO
certificare
riscuri
uitare
drept
conduita
operator
consiliere
DPIA
cerere acces
transfer
termen
auditare drepturi
persoana identificata
date biometrice
internet
masuri adecvate
acces
online
legalitate
evaluare
confidential
drept de acces
imputernicit
DataProtection
Legea 677
consimtamant
drepturi copii
20.000.000 euro
date speciale
legislatie
localizare
incident
informatii
planuri
management
date personale
control
GPS
scop

Conștientizare

Informare

Instruire

Consiliere

Planificare

Analiză

Proiectare

Implementare

Testare

Monitorizare

Securitatea prelucrărilor de date, pe scurt:

Art. 5

Datele cu caracter personal sunt prelucrate într-un mod care asigură **securitatea adecvată** a acestora, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("*integritate şi confidenţialitate*").

1111111111111111

Art. 24

Responsabilitatea operatorului

Operatorul pune în aplicare **măsuri tehnice şi organizatorice adecvate** pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.

Securitatea prelucrărilor de date, pe scurt:

Secţiunea 2
<u>Securitatea</u> datelor cu caracter personal

Măsuri tehnice şi organizatorice adecvate:

- **pseudonimizarea** şi **criptarea** datelor cu caracter personal;
- capacitatea de a asigura **confidenţialitatea**, **integritatea**, **disponibilitatea** şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare;
- capacitatea de a **restabili** disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru **testarea**, **evaluarea** şi aprecierea periodică a eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

Securitatea prelucrărilor de date, pe scurt:

Art. 33: Notificarea autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal

Când are loc o încălcare a securităţii datelor cu caracter personal, operatorul notifică acest lucru autorităţii de supraveghere competente în termen de **cel mult 72 de ore** de la data la care a luat cunoştinţă de aceasta.

Notificarea conține cel puțin:

- categoriile şi numărul înregistrărilor de **date** și al persoanelor vizate în cauză;
- numele şi datele de **contact** ale responsabilului cu protecţia datelor sau un alt punct de contact al operatorului;
- **consecinţele** probabile ale încălcării securităţii datelor cu caracter personal;
- **măsurile** luate sau propuse spre a fi luate de operator pentru a remedia incidentul, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Securitatea prelucrărilor de date, pe scurt:

Art. 34: <u>Informarea</u> persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal

- În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată **fără întârzieri** nejustificate cu privire la această încălcare.

- Informarea conține o **descriere** într-un limbaj clar şi simplu a caracterului încălcării securităţii datelor cu caracter personal, precum şi cel puţin informaţiile şi măsurile menţionate la articolul 33 alineatul (3) literele (b), (c) şi (d), respectiv: date de contact, consecințe și măsuri de remediere.

Date privind sănătatea, date genetice, date biometrice

Potrivit art. 9, următoarele informații fac parte din categoriile <u>speciale</u> de date cu caracter personal:

- **date privind sănătatea** - date legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

- **date genetice -** date referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective;

- **date biometrice** - date referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane.

Date privind sănătatea, date genetice, date biometrice

Prelucrarea date biometrice, genetice sau referitoare la sănătate **este interzisă**, cu excepțiile următoare:

- când persoana vizată şi-a dat **consimţământul explicit**;
- pentru **protejarea intereselor vitale** ale persoanei vizate (aflată în incapacitate fizică pentru a-și da consimțământul);
- în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacităţii de muncă a angajatului, de stabilirea unui **diagnostic medical**, de furnizarea de **asistenţă medicală** sau socială sau a unui **tratament medical** sau de gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială (*de către un profesionist supus obligaţiei de păstrare a secretului profesional*);
- când prelucrarea este necesară din motive de interes public în domeniul **sănătăţii publice**.

Date privind sănătatea, date genetice, date biometrice

Alte aspecte specifice legate de prelucrarea datelor privind sănătatea, a datelor genetice sau a datelor biometrice:

- Desemnarea unui **responsabil cu protecţia datelor** (DPO);
- Notificarea ANSPDCP cu privire la prelucrarea datelor cu caracter personal privind sănătatea, date biometrice sau date genetice (potrivit cu ***DECIZIA nr. 200/2015*** *privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea*);
- Categoriile speciale de date cu caracter personal necesită ***un nivel mai ridicat de protecţie*;**
- Statele membre pot menţine sau introduce condiţii suplimentare, inclusiv restricţii, în ceea ce priveşte prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea.

Condiţii generale pentru impunerea amenzilor administrative (*extras*)

Până la **10 000 000 EUR** sau până la **2%** din cifra de afaceri totală anuală, pentru încălcarea dispozițiilor referitoare la:

- Condiţiile aplicabile la **consimţământul** copiilor;
- Prelucrarea de categorii **speciale** de date cu caracter personal;
- Întocmirea e**videnţe**i cu activităţilor de prelucrare;
- **Securitatea** datelor cu caracter personal;
- Evaluarea **impactului** asupra protecţiei datelor şi consultarea prealabilă.

Până la **20 000 000 EUR** sau până **4%** din cifra de afaceri totală anuală, pentru încălcarea dispozițiilor referitoare la:

- **Principii**le legate de prelucrarea datelor cu caracter personal ("legalitate, echitate şi transparenţă");
- Condiţii privind **consimţământul**;
- **Drepturile** persoanei vizate (transparență, informare, dreptul de acces, opoziție, portabilitate etc.);
- **Transferurile** de date cu caracter personal în străinătate.

Diverse considerații

GDPR poate presupune alocarea de noi resurse și investiții bănești. Dar, aduce și avantaje, cum ar fi:

- ❖ simplificarea și armonizarea la nivel juridic și administrativ a protecției datelor în Uniunea Europeană. Facilitează libera circulație a datelor personale în spațiul european;
- ❖ responsabilizarea operatorilor cu privire la prelucrările proprii de date și informații;
- ❖ stimularea inovației pentru tehnologiile care asigură stocarea și protecția datelor.

Statistic, se dezvoltă un milion de noi feluri de malware în fiecare zi. Astăzi, timpul mediu în care un malware stă nedetectat într-o organizație este de 201 zile (conf. Ponemon Institute).

GDPR își propune să pregătească operatorii pentru un viitor în care informația devine critică pentru supraviețuirea noastră. Într-o societate marcată de atacuri cibernetice și teroriste, cu cât entitățile colectează și distribuie mai multe date despre oameni, cu atât expunerea potențială crește exponențial.

Securitatea prelucrărilor de date, pe scurt:

Cateva consideratii …
(Ref. Cyber security report publicat pe site-ul https://www.cnbc.com)

“There's no such thing as an impenetrable system, but often even a half-decent defense will deter many cybercriminals — they'll move on and look for an easier target”.

“Criminals are getting better, faster and nobody on the defensive is getting better fast enough”.

“Most hacks take minutes to do — and weeks to discover”.

“The study found that US companies took an average of 206 days to detect a data breach”.

“With the availability of personal details available on social media, phishing emails are better camouflaged than ever”.

“Even if your technology is tightly-controlled, people remain easy to fool”

“Once a phishing email is sent, it takes only about 1 minute and 40 seconds before the first user takes the bait”

Scurgeri de Informatii ...

RAPORT

cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2016

În 2016, CERT-RO a colectat și procesat **110.194.890** de alerte de securitate cibernetică, ***în creștere cu 61,55% față de anul 2015*** (68.206.856), dintre care:

- 38% (2,9 milioane) dintre adresele IP publice din România au înregistrat cel puțin o alertă;
- 81% (89 milioane) dintre alerte se referă la sisteme sau servicii vulnerabile;
- 13% (14 milioane) dintre alerte se referă la sisteme infectate cu malware de tip botnet;
- 639 de domenii web „.RO” au fost utilizate de site-uri web compromise.

Măsuri de prevenire a incidentelor de securitate:

- **Securizarea terminalelor** (stații de lucru, telefoane, tablete etc.) prin utilizarea unor soluții/tehnologii de tip antivirus/ antimalware, sandbox și de criptare a datelor;
- **Securizarea infrastructurii de rețea** prin utilizarea unor soluții/ tehnologii de protecție perimetrală (ex. firewall);
- **Monitorizarea continuă** a fluxurilor de date în cadrul infrastructurii IT prin utilizarea unor soluții/tehnologii specifice;
- Implementarea unor măsuri adecvate de **securitate fizică** în spațiile unde sunt procesate sau depozitate cantități mari de date;
- **Limitarea accesului** utilizatorilor la resurse și la date în baza atribuțiilor acestora (principiul "*nevoia de a cunoaște*");

Măsuri de prevenire a incidentelor de securitate:

- Implementarea unei proceduri adecvate de **backup** (copii de siguranță) care să includă și verificarea periodică a integrității datelor și a procesului de restaurare;
- Implementarea unei **politici de securitate** care să fie asumată și respectată de toți utilizatorii;
- Utilizarea unor **proceduri de răspuns** la incidentele de securitate și de gestionare a vulnerabilităților;
- Dispunerea de **personal adecvat** pentru securizarea infrastructurii IT și pentru a răspunde la incidentele de securitate;
- **Instruirea periodică** a personalului cu privire la riscurile, amenințările și vulnerabilitățile de securitate; fișa postului actualizată;
- Realizarea de **audituri/evaluări** periodice de securitate a infrastructurii IT, a personalului și a procedurilor.