BIO MED 2023

LES JOURNÉES POUR L'AVENIR DE LA BIOLOGIE MÉDICALE

9 & 10 MARS 2023 • Palais des Congrès de Paris Porte Maillot

La Cybersécurité, un enjeu majeur pour tous les acteurs de la biologie médicale aujourd'hui

Alexandre Rousseaux

Business Development Manager

BYG4lab®

UNE VÉRITABLE TEMPÊTE CYBER

La digitalisation et l'interconnexion des systèmes s'accélèrent à un rythme plus élevé que la sécurisation de l'écosystème informatique.

Les établissements de santé constituent une cible de choix

- Les données de santé sont les plus lucratives pour les cybercriminels
- Le coût d'un dossier médical est 50 fois élevé qu'un dossier bancaire sur le dark web
- 730 déclarations d'incidents en 2022 pour les hôpitaux publics
- 3e place des cibles privilégiées des pirates (10% des rançongiciels traités ou rapportés à l'Anssi en 2022)

TYPES DE CYBER-ATTAQUES

Accès non autorisé

- Interception du flux de données par un individu malveillant qui peut alors les conserver, les modifier, voire les crypter.

Logiciel malveillant (malware)

- Programme destiné à perturber les fonctionnalités du logiciel de DMDIV, pouvant entraîner une perte de contrôle, un ralentissement, etc.

Attaques par « déni de service »

- Surcharge de requêtes faites au logiciel de DMDIV entraînant une interruption du service ayant pour conséquence un ralentissement ou un blocage complet du système.

LES PRINCIPES FONDAMENTAUX DE LA CYBERSÉCURITÉ

Disponibilité

- Pouvoir toujours accéder aux données peu importe le lieu de stockage.

Intégrité

- Les informations sont transmises entre un émetteur et un destinataire ne peuvent pas être altérées.

Confidentialité

- Les informations transmises entre un émetteur et un destinataire ne peuvent être lues que par l'émetteur et le destinataire (qui peuvent être des êtres humains ou des machines).

Authentification

- Toute identité (d'une personne ou d'une machine) doit être vérifiée.

Non répudiation

- Garantie qu'un accord ne peut pas être nié (exemple de la signature électronique)

LE POSITIONNEMENT DU MIDDLEWARE

	PRE ANALYTIQUE	ANALYTIQUE	POST ANALYTIQUE
“ Le dossier “ **SIL**	Démographie Connectivité H.I.S. Entrée des commandes		Validation clinique Diffusion des résultats - Papier - Server - S.I.H - Facturation
“ L’échantillon ” **DATA MANAGEMENT**	Suivi des échantillons Flux de travail pré-analytique	Connexion des instruments Validation (règles d’expertise) Lots CQ Solution d'automatisation Solution de préparation des échantillons Workflow technique Indicateurs / Alertes Validation de la méthode Épidémiologie	Traçabilité complète Surveillance post-marché B.I Épidémiologie Hygiène
“ Le test ” **INSTRUMENT**	Calibration Maintenance Préparation	Gestion des stocks Réactifs Flags analytiques Tests réflexes	

BYG4lab®

L'IMPORTANCE DU DATA MANAGEMENT

Le Data Management devient un facteur clé de succès dans l'organisation du laboratoire

- Augmentation de la charge de travail
- Nécessité d'être plus spécifique que le SIL
- Nécessité d'un suivi transversal
- Complexité croissante des solutions
- Des exigences réglementaires croissantes
- Besoin d'agilité et d'ouverture

BYG4lab®

BYG4LAB EN QUELQUES MOTS

Leader européen dédié aux solutions de Middleware et data management

40 ans

~ 90 collaborateurs

~ 350 drivers instruments

~ 4000 Stations de travail WW

~ 500 Solutions de Data Management

(toutes disciplines – jusqu'à 90 inst. connectés sur 1 seule solution)

CoreLab

Microbiologie

EBMD (POC)

BYG4lab®

BIO MED 2023

UNE SUITE LOGICIELLE MULTIDISCIPLINAIRE COMPLÈTE

M.D.M byBYG®

Le premier Master Data Management de la biologie médicale.

nYna®	Solution de Data Management dédiée à la gestion de la production et de la qualité.
pocY®	Solution de Data Management dédiée à la gestion des EBMD.
pYlotR	Solution de gestion des activités de microbiologie.
Ynfectio®	Solution experte d'épidémiologie et d'hygiène.
qualYnk®	Système expert de gestion du contrôle qualité.

B.I byBYG®

La Business Intelligence adaptée à la biologie médicale.

YlineR

UNE ACHITECTURE TECHNIQUE FULLWEB, INNOVANTE & UNIQUE

LA CYBERSÉCURITÉ, UN ENJEU MAJEUR MAIS CONCRÈTEMENT

Un suivi normatif

- Les normes et règlementations applicables, les analyses des risques

Des choix technologiques et des processus internes adaptés

- L'architecture de nos solutions (indépendance des couches logiciel)
- Les technologies mises en œuvre (Back, Front , BDD, sécurisation des communications)
- Les pratiques de développement – Audit et tests

Des fonctionnalités développées en lien direct avec la protection des données

- Droits, traçabilité…

Des outils adaptés

- Développement logiciel
- Installation
- Maintenance et mise à jour

BYG4lab®

LE NORMATIF (1/3)

Système de Management de la Qualité

- Prise en compte de la cybersécurité dans le Système de Management de la Qualité
- ISO 13485 - Dispositifs médicaux

Cycle de vie du logiciel

- Prise en compte de la cybersécurité dans nos applications dès la conception puis tout au long de leur cycle de vie. Garantir la confidentialité / l'intégrité des données / l'auditabilité de nos applications
  - IEC 62304 - Logiciels de dispositifs médicaux — Processus du cycle de vie du logiciel
  - IEC 82304-1 - Logiciels de santé : Exigences générales pour la sécurité des produits
  - RGPD - Règlement général sur la protection des données
    - Privacy by Design (protection des données personnelles dans vos systèmes IT)
    - Privacy by Default (standard de protection appliquées par défaut)
  - MDCG 2019-16 : Guidance on Cybersecurity for medical devices
  - CLSI AUTO 11-A - IT Security of In Vitro Diagnostic Instruments and Software Systems
  - (21 CFR Part 11 - intégrité des données électroniques)

LE NORMATIF (2/3)

Gestion des risques

- Identification / Maitrise / suivi des risques de cybersécurité pouvant aboutir à un dommage sur les données sensibles et/ou patients
- Adaptation des fonctionnalités pour la maitrise des risques identifiés
  - ISO 14971 - Application de la gestion des risques aux dispositifs médicaux
  - IEC 62366-1 - Application de l'ingénierie de l'aptitude à l'utilisation aux dispositifs médicaux

Sécurisation de l'environnement de travail

- Sécurisation des connexions en télémaintenance
  - CLSI AUTO 9 - Remote Access to Clinical Laboratory Diagnostic Devices via the Internet
  - PGSSI-S
  - Utilisation de solution de télémaintenance avec cryptage des données ou solution de connexion du client
  - Accès en télémaintenance tracés dans rapport intervention
- Politique informatique interne
  - Respect du guide d'hygiène informatique ANSSI pour nos postes de travail et serveurs
  - Plans de continuité et de reprise d'activité (PCA/PRA)

LE NORMATIF (3/3)

Surveillance régulière des composantes et unités logicielles du système

- Logiciels non développés par BYG4lab (SOUPs)
  (Ex : MariaDB, .net Core, Angular, Entity Framework etc…)
  - Analyse récurrente de la criticité de chacun des SOUP
  - Suivi des vulnérabilités et analyse d'impacts des défaillances identifiées et de leur acceptabilité
  - Mise en place d'une fiche de test permettant de valider le SOUP
- Caractérisation du système
  - Software Bills of Materials (SBOM)

SÉCURITÉ DÈS LA CONCEPTION (SECURITY BY DESIGN)

Intégrer la sécurité dès la phase de conception

- Evaluation des risques pour chaque choix technologique ou pour chaque évolution (architecture, outils, code, fonctionnalité, BDD)
- Gérer l'obsolescence de composants et de stacks logiciels ou simplement en prévoyant la fin de vie d'une application utilisée (road map de mise à jour)

Actions

- Analyse de risques logiciel
- Revue des spécifications fonctionnelles et techniques
- Analyse de la qualité du code
- Formation et sensibilisation des développeurs
- Inspection de l'implémentation par les experts techniques
- Audit de sécurité et/ou de pénétration

CHOIX TECHNOLOGIQUES RESPECTANT L'ÉTAT DE L'ART

Sécurité

- Architecture en couche (Back, Front, ORM = communication avec la BDD)
- L'ensemble des couches disposent d'une communication sécurisée
  - HTTPS (http + couche de chiffrement)
  - SSL (protocole de sécurisation de la couche transport

Front

Application BYG4lab®

Un ou plusieurs modules
- module 1
- module 2
- module 3

Modules transversaux
- Fondation

Composants graphiques
- Composant

Back

Contrôleur

Domaine

Infrastructure

BYG4lab®

OUTILS ET FRAMEWORK DE DÉVELOPPEMENT

VISUAL STUDIO

- Environnement de développement fourni par **Microsoft**
- **Mises à jour régulières** assurent une correction rapide et préventive des potentielles failles

.Net Core 3.1 (migration 6.0)

- Framework de développement fourni par **Microsoft**
- **Mises à jour régulières** permettant de disposer de fonctions natives pour sécuriser l'application
- **Vulnérabilités corrigées** de façon pro-active et régulière par Microsoft
- **Communauté importante et active**

Angular 13

- Framework de développement fourni par **Google**
- **Mises à jour régulières** du framework permettant de disposer de **fonctions natives de cybersécurité pour les applications WEB**
- **Communauté importante et active**

Entity Framework

- **Ajoute une couche de sécurité supplémentaire** (ex. Injection SQL)
- Mises à jour régulières de **Microsoft** permettant de **disposer des fonctions natives pour sécuriser l'application**

Services Windows

- Une sécurité accrue conforme à l'état de l'art
- Evite d'avoir une session Windows Server en auto-logon (.exe = faille de sécurité)
- Monitoring et déploiement intégrés à l'OS

OUTILS / BASE DE DONNÉES : MARIADB

Intègre un chiffrement natif des données avec une gestion flexible des clés

Mises à jour régulières portées par une communauté importante et très active

Haute disponibilité : possibilité de réplication, clustering et basculement automatique pour assurer une continuité de service importante.

OUTIL D'ANALYSE DE LA STRUCTURATION DU CODE

En plus de s'appuyer sur des frameworks récents, BYG4lab a défini et mis en œuvre des bonnes pratiques de programmation.

La qualité du code (maintenabilité, sécurité, suivi des bonnes pratiques) est suivie via l'outil SonarQube.

sonarqube

IDENTIFICATION SUR NOS APPLICATIONS

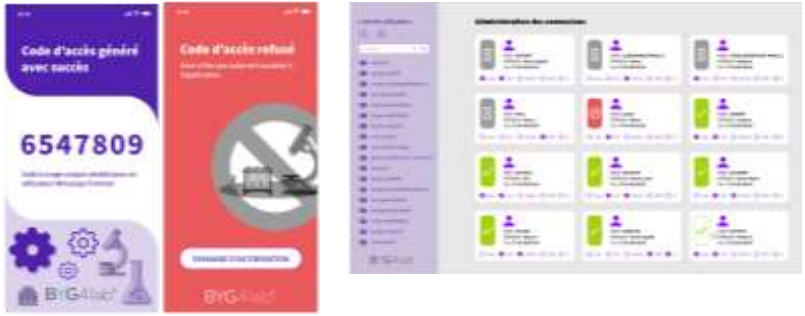
Politique renforcée de gestion des mots de passe

- Couple identifiant / mot de passe unique
- Règles de complexité du mot de passe à respecter
- Gestion de l'obsolescence des mots de passe
- Règle du moindre privilège
- Déconnexion automatique
- Authentification à 2 facteurs pour les ingénieurs BYG

Gestion du SSO (ou « Single Sign-On »)

- Authentification unique pour l'utilisateur
- Renforcement des politiques de mots de passe
- Déploiement facilité de technologies d'authentification multi-facteur et adaptative.

IDENTIFICATION TECHNICIENS BYG4LAB



- techidentitY est un outil dédié à nos techniciens
- Permet une identification sécurisée et privilégiée à nos applications et outils d'administration
- Gestion en temps réel des autorisations d'accès à nos solutions via un portail WEB
- Chaque intervenant est identifié avec des droits d'accès définis (moindre privilège)
- Traçabilité totale des actions réalisées par chaque intervenant

BYG4lab®

SURVEILLANCE ET GESTION POST-COMMERCIALISATION

Mise en place d'un process de surveillance post-commercialisation pour gérer les vulnérabilités et les menaces de cybersécurité.

- Recueil
  - tests interne, remontées clients, veille (National Vulnerability Database, éditeurs)
- Analyse et évaluation
- Si nécessaire, définition de mesure de maitrise des risques ou de compensation des vulnérabilités
  - stratégie de patching

MERCI DE VOTRE ATTENTION

BYG4lab®

Stand 29

Contact :

BYG4lab®
+33 (0) 5 34 25 07 10

Localisation :

13, rue d'Ariane
31240 L'Union
FRANCE

Social media :

www.byg4lab.com
@BYG4lab®
BYG4lab® / YouTube