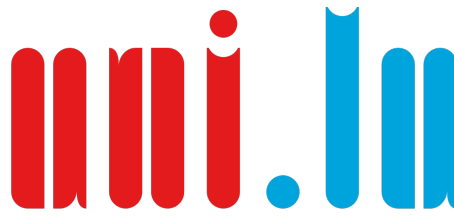


Analyse et évaluation de sécurité dans le cadre des
mises à jour et correctifs des systèmes d'exploitation
en industrie pharmaceutique

Bob MULUMBA TUBADI

Année académique 2017-2018 - Promotion 8

Version : Draft Final



UNIVERSITÉ DU
LUXEMBOURG

Faculté des Sciences, de la Technologie et de la Communication (FSTC)

Master en Management de la Sécurité des Systèmes d'Information
Année académique 2017-2018 - Promotion 8

**Analyse et évaluation de sécurité dans le cadre
des mises à jour et correctifs des systèmes
d'exploitation en industrie pharmaceutique**

Bob MULUMBA TUBADI

*Responsable
académique*

Nicolas MAYER, PhD
Senior R&T Associate
Luxembourg Institute of Science and Technology

Responsable local

Cecile MIGNON
Senior Manager
GlaxoSmithKline Vaccines

Bob MULUMBA TUBADI

*Analyse et évaluation de sécurité dans le cadre des mises à jour et correctifs des systèmes
d'exploitation en industrie pharmaceutique*

Master en Management de la Sécurité des Systèmes d'Information

Responsable académique : Nicolas MAYER, PhD

Responsable local : Cecile MIGNON

Université du Luxembourg

Faculté des Sciences, de la Technologie et de la Communication (FSTC)

2, avenue de l'Université

L-4365 Esch-sur-Alzette

Résumé

Nous vivons dans un monde où les systèmes de contrôle et de fabrication industrielle modernes sont de plus en plus complexes, numériques et connectés.

Dans le passé, ces technologies étaient isolées d'autres réseaux, les opérations d'aujourd'hui exigent généralement que les données soient transférées entre les réseaux industriels et externes.

Tout logiciel, utilisé à cette fin, est sujet à des vulnérabilités techniques. Une fois découverte et partagée publiquement, ces vulnérabilités peuvent être exploités rapidement par les cybercriminels et exposent les entreprises à des risques.

Les pirates informatiques peuvent tirer parti des vulnérabilités connues dans les systèmes d'exploitation ou les applications tierces, si les mises-à-jour ne sont pas correctement implémentées. Avec pour but de perturber les systèmes de contrôle et les infrastructures dépendantes.

Ce mémoire décrit la complexité des systèmes d'information et de contrôle industriels typiques dans le secteur pharmaceutique. Avec une analyse et évaluation de sécurité dans le cadre de la gestion des mises à jour et correctifs au niveau des systèmes d'exploitation.

L'ensemble dans le but de maîtriser au mieux la sécurité dans les systèmes critiques pharmaceutiques de type opérationnel.

Mots clés : Sécurité, Patching, Systèmes d'exploitation, Systèmes industriels, Sociétés pharmaceutiques, Méthodologies de gestion de risques, Technologie de l'information (IT), Technologie opérationnelle (OT)

Abstract

We live in a world where modern control systems are increasingly complex, digital and connected.

In the past, these technologies have been isolated from other networks, today's operators generally require that data be transferred between industrial and external networks.

Any software, in use for that purpose, is prone to technical vulnerabilities. Once discovered and shared publicly.

These pitfalls can rapidly be exploited by cybercriminals and exposes organisations to risk that hackers can take advantage of known vulnerabilities in operating systems and third-party applications, if they are not properly patched or updated and disrupt real-time control systems and dependent infrastructures.

This master thesis describes different types of information and industrial control systems in the pharmaceutical sector. It proposes a security analysis based on a comparison of existing methods chosen for operating systems security patches.

All in order to provide better security on the perspective of a critical pharmaceutical industrial system.

Keywords : Security, Patching, Industrial operating systems, Pharmaceutical companies, Risk management frameworks, Information technology (IT), Operational technology (OT)

Déclaration d'honnêteté

Je déclare et confirme avoir réalisé ce mémoire sans l'aide illicite d'autrui et en me conformant aux règles d'honnêteté intellectuelle.

Esch-sur-Alzette, 4 septembre 2018

Bob MULUMBA TUBADI

Remerciements

Mes remerciements s'adressent à ma famille pour la patience et l'appui pendant ces années d'études. Leur soutien a été indéfectible tout au long de ce long processus d'apprentissage aussi bien au niveau des cours que lors de l'écriture de ce mémoire.

Je désire remercier mon responsable académique (Nicolas MAYER, PhD) pour la rigueur scientifique, les judicieux conseils, son expérience dans le domaine de la sécurité et sa patience qui m'ont stimulé lors de la réalisation de ce travail.

Je remercie mon responsable local (Cecile MIGNON, Senior Manager) pour le soutien moral adressé et pour m'avoir permis de mettre en pratique les aspects liés à ce cursus dans le cadre de mon travail quotidien.

Enfin, un grand merci à toutes les personnes (Professeurs, collègues et amis) qui m'ont supporté, dans tous les sens du terme, pendant ce programme d'étude.

Table des matières

1	Introduction	1
1.1	Présentation	2
1.2	Contexte	5
1.3	Motivation et problématique	6
1.4	Objectifs et organisation du mémoire	8
2	Cadre théorique - État de l'art des connaissances	10
2.1	Contexte industriel pharmaceutique et systèmes d'information industriels	10
2.1.1	Types de départements	12
2.1.2	Architecture et terminologie	14
2.1.3	Utilisation	17
2.1.4	Cycle de vie	18
2.1.5	Limites	18
2.2	Logiciels industriels	19
2.2.1	Types de systèmes d'exploitation	20
2.2.2	Types de logiciels (COTS)	23
2.2.3	Types de logiciels (non-COTS)	24
2.3	Concepts de risques et contrôles	26
2.3.1	Risques de sécurité	26
2.3.2	Contrôles de sécurité	29
2.3.3	Ressources pour des contrôles de sécurité de qualité	31
2.3.4	Menaces, impacts et ressources pour des contrôles de sécurité de qualité	36
2.4	Vulnérabilités	37
2.4.1	Types de vulnérabilités	39
2.4.2	Cycle de vie des vulnérabilités	41
2.4.3	Métriques des vulnérabilités et indices d'exploitabilité	42
2.5	Patching, mises à jour et correctifs	46
2.5.1	Types de patches	47
2.5.2	Gestion des patches	49
2.6	Matrices des responsabilités	52
2.7	Conclusion	53

3	Analyse des difficultés du patching dans le secteur pharmaceutique	54
3.1	Différences entre IT vs OT	56
3.2	Comparaison des méthodologies	66
3.2.1	Health Information Trust Alliance (HITRUST)	68
3.2.2	International Society of Automation (ISA)	70
3.2.3	International Organization for Standardization (ISO)	71
3.2.4	North American Electric Reliability Corporation (NERC)	74
3.2.5	National Institute of Standards and Technology (NIST)	76
3.2.6	Tableau récapitulatif	77
3.3	Conclusion	79
4	Cadre pratique - Mise en pratique en contexte local	82
4.1	Contexte d'analyse et d'évaluation	82
4.1.1	Notre approche méthodologique	84
4.2	Gestion des risques dans le cadre d'un contexte pharmaceutique complexe	87
4.3	(Phases 1-3) - Évaluation des risques	88
4.3.1	1 - Établissement du contexte	88
4.3.2	2 - Identification et estimation des actifs	90
4.3.3	3 - Évaluation des menaces et des vulnérabilités	93
4.4	(Phase 4) - Traitement des risques	98
4.4.1	Plan de traitement des risques	99
4.4.2	Analyse des risques résiduels	102
4.4.3	Acceptation des risques critiques	102
4.5	(Phase 5) - Surveillance et réexamen des risques	103
4.6	Plan d'implémentation d'une stratégie de patching des systèmes d'exploitation	104
4.7	Conclusion	108
5	Conclusion générale	110
5.1	Améliorations futures	113
6	Glossaire	114
7	Définitions	116
	Bibliographie	118

Table des figures

1.1	Vulnérabilités déclarées depuis 2010 - (Source : ICS-CERT)	2
1.2	Ransomwares en 2017 - (Source : NTT)	3
1.3	Vue d'ensemble et comparaison des cybermenaces en 2017 - (Source : ENISA)	4
1.4	Secteurs d'activités de GlaxoSmithKline - (Source : GSK)	5
1.5	Secteurs d'activités et la cadence des correctifs - (Source : US Federal Government)	7
2.1	Régulateurs et standards GxP - (Source : GSK)	11
2.2	Cycle de vie R&D et GIO - (Source : Sanofi)	13
2.3	Structure des installations dans l'OT - (Source : ISA)	14
2.4	Modèle logique hiérarchique de PERA : IT vs OT - (Source : ISA)	15
2.5	Computer System vs Computerized System - (Source : GSK)	17
2.6	Système et validation des équipements - (Source : Sanofi)	17
2.7	Types de logiciels industriels - (Source : GSK)	19
2.8	Relations dans un système d'exploitation moderne - (Source : Wikipedia)	20
2.9	Principaux systèmes d'exploitation en OT - (Source : Wikipedia)	22
2.10	Logiciels COTS en environnement pharmaceutique - (Source : Personnel)	24
2.11	Taxonomie dans la catégorie des contrôles du risque - (Source : HITRUST)	30
2.12	Modèles de divulgation des vulnérabilités - (Source : Symantec)	41
3.1	Menaces, vulnérabilités et mesures - (Source : WEF)	54
3.2	Facteurs d'influence entre IT et OT - (Source : ISA)	56
3.3	État convergence entre IT et OT - (Source : ISA)	57
3.4	Facteurs d'influence de sécurité entre IT et OT (GIO) - (Source : FDA) .	58
3.5	Facteurs d'influence entre IT et OT (RD) - (Source : FDA)	58
3.6	Modèle Parkerian Hexad - (Source : Donn B. Parker)	59
3.7	Intégration des systèmes - (Source : Personnel)	60
3.8	Relation entre risques (RD) - (Source : FDA)	66
3.9	Normes ISA - (Source : ANSI/ISA)	70
3.10	Structure ISO - (Source : ISO)	71
3.11	Résultat Comparatif normes et publications de sécurité - (Source : T.U.T)	73
3.12	Comparatif normes et publications de sécurité - (Source : T.U.T)	73
3.13	Normes NERC - (Source : NERC)	74
3.14	Structure NIST - (Source : NIST)	76

3.15	Adaptabilité de la méthodologie PDCA selon HITRUST - (Source : Personnel)	79
4.1	Plan de gestion de risques avec Sécurité et Sûreté - (Source : BSI) . . .	83
4.2	Gestion des risques IT/OT en milieu pharmaceutique - (Source : HITRUST)	86
4.3	Plan de gestion de risques adapté - (Source : Personnel)	87
4.4	Relations entre les concepts de sécurité et sûreté - (Source : Personnel)	89
4.5	Scénario de risques et impacts - (Source : Personnel)	94
4.6	Plan de gestion de risques adapté au patching - (Source : Personnel) .	107

Liste des tableaux

2.1	Méthodologie de contrôles en secteur pharmaceutique - (Source : HIMSS)	31
2.2	Types de menaces - (Source : Coursera)	37
2.3	Catégorie des cybercriminels - (Source : Coursera)	37
2.4	Catégories de vulnérabilités - (Source : Coursera)	38
2.5	Catégorie de métrique CVSS - (Source : CVE)	43
2.6	Évaluation de l'indice d'exploitabilité	44
3.1	Perspectives de confidentialité entre IT vs OT - (Source : Personnel)	62
3.2	Perspectives d'intégrité entre IT vs OT - (Source : Personnel)	62
3.3	Perspectives de disponibilité entre IT vs OT - (Source : Personnel)	62
3.4	Perspectives de la maintenabilité IT vs OT (1) - (Source : Personnel)	63
3.5	Perspectives de la maintenabilité IT vs OT (2) - (Source : Personnel)	63
3.6	Perspectives de la maintenabilité IT vs OT (3) - (Source : Personnel)	63
3.7	Perspectives de sûreté IT vs OT - (Source : Personnel)	64
3.8	Perspectives de fiabilité IT vs OT - (Source : Personnel)	64
3.9	Perspectives additionnelles IT vs OT - (Source : Personnel)	64
3.10	Comparatif normes et publications de sécurité - (Source : Personnel)	78
4.1	Scénarios de risques - (Source : Personnel)	85
4.2	Exemple d'identification d'actifs - (Source : Personnel)	91
4.3	Matrice de criticité des activités et valeur des actifs - (Source : Personnel)	92
4.4	Critères d'impact - (Source : Personnel)	95
4.5	Échelle des probabilités - (Source : Personnel)	95
4.6	Matrice de tolérance des risques - (Source : Personnel)	95
4.7	Évaluation des risques - (Source : Personnel)	97
4.8	Plan de traitement des risques - (Source : Personnel)	101
4.9	Plan d'exécution du patching - (Source : Personnel)	105