مجلة الادارة والتنمية للبحوث والدراسات

المجلد 12 / العـدد: 01 جوان (2023)،
ص 213– 232

دور الأمن المعلوماتي في مواجهة المخاطر التي تهدد نظام معلومات المؤسسة

دراسة حالة مؤسسة الإنجازات الكهربائية REELEC

The role of information security in facing the risks that threaten the enterprise information system REELEC case study

عبد الوهاب بوبعة[1]* **لعور عبد العالي [2]**

[1] المركز الجامعي تيبازة (الجزائر)، boubaaa03@gmail.com

[2] المركز الجامعي تيبازة (الجزائر)، laour.abdelali@cu-tipaza.dz

تاريخ الاستلام: 19 /2023/01 تاريخ القبول: 2023/03/19 تاريخ النشر: 2023/06/01

ملخص: تهدف هذه الدارسة إلى إبراز دور التطورات الحاصلة في تكنولوجيا المعلومات والاتصالات والتي تشهد تغيرات متسارعة في كافة الميادين، في تغيير طرق ووسائل تنفيذ الأنشطة، إذ أصبحت عملية انتقال المعلومة وتدفقها عبر الشبكات إحدى علامات الاقتصاد الرقمي الجديد، من خلال تطوير أساليب المعالجة، التخزين والتوزيع. كل هذا أدى إلى تطوير أنظمة معلومات المؤسسة، كما تهدف الدارسة إلى الكشف عن المخاطر المعلوماتية التي تهدد أمن وسلامة المعلومات من خلال مختلف الاعتداءات الالكترونية.

من بين أهم النتائج المتوصل إليها هو أنه يجب على المؤسسة التيقظ والعمل على توفير الأمن والحماية اللازمين لنظم معلوماتها بمساعدة مجموعة من الوسائل التقنية والتنظيمية، التي تضمن سريتها، سلامتها وموثوقيتها، خصوصا وأنها تنشط في ظل اقتصاد شعاره "من يملك المعلومة يملك السيطرة".

كلمات مفتاحية: نظام معلومات المؤسسة، المخاطر المعلوماتية، أمن نظم المعلومات

تصنيف JEL: XN1, XN2

Abstract:

This study aims to highlight the role of ICT have brought about changes in all fields, through changes in the ways and means of implementing

* **المؤلف المرسل**

activities, the transmission and flow of information through networks has become one of the signs of the new digital economy, by the development of processing methods, storage and distribution of information. All this led to the development of enterprise information systems, which increased information risks that threaten the security and integrity of information through various forms of cyber-attacks.

It has therefore become necessary to be vigilant and work to provide the necessary security and protection for its information systems, using a range of technical and organizational means, which ensure their confidentiality, safety and reliability, especially as it activate in the economy where "Whoever owns the information owns the control".

Keywords: Enterprise information system, information risks, information systems security.

Jel Classification Codes: XN1, XN2.

1.مقدمة

عرف العالم في السنوات الأخيرة تطورات جد متسارعة في تكنولوجيا المعلومات والاتصالات، مما أدى لإحداث عدة تغيرات في الممارسات اليومية للأفراد، المؤسسات وحتى الحكومات، حيث أصبحت المعلومة تتداول مثلها مثل السلع والخدمات.

أصبحت المؤسسات في الوقت الحالي تولي اهتمام كبير بنظام المعلومات باعتباره أداة تسمح بالتحكم في المعلومة (حيازة، المعالجة، التخزين، التدفق...)، وبالتالي الرفع من أداء المؤسسات ودعم مزاياها التنافسية، لكن سوء استخدامها لنظام المعلومات و/أو غياب الأمن المعلوماتي، خاصة في ظل تنوع وتعدد المخاطر المعلوماتية والتي تعود بالسلب عليها. وعليه أصبح من الضروري على المؤسسات وضع إجراءات أمن نظام المعلومات والعمل على تطبيقها وتطويرها.

من خلال ما سبق، يمكن **طرح الاشكالية التالية** " فيما يتمثل الدور الارتكازي الذي يلعبه أمن المعلومات في مواجهة المخاطر التي تهدد نظام معلومات المؤسسة، وما هي أهم إجراءات أمن نظام المعلومات التي يجب على المؤسسة الالتزام بها؟"، كما **تهدف هذه الدراسة** إلى:

- إبراز المكونات الأساسية لنظام المعلومات.

- الكشف عن مخاطر أمن المعلومات في المؤسسة.
- توضيح أشكال الاعتداءات المعلوماتية.
- تحديد مجالات الامن المعلوماتي في المؤسسات الجزائرية وفق المرجعية الوطنية لأمن المعلومة.
- توضيح معايير أمن نظم المعلومات.
- عرض للإجراءات الأمنية المتخذة على مستوى مؤسسة الإنجازات الكهربائية EPE REELEC SPA، في إطار تأمين نظام معلوماتها.

سوف نستخدم في **هذه الدراسة المنهج** الوصفي والمنهج التحليلي.

1- تعريف نظام معلومات المؤسسة

تعددت التعاريف حول نظام معلومات المؤسسة بسبب تنوع مكوناته، مهامه وأهميته، سنحاول في هذا العنصر عرض بعض التعاريف:

- مجموعة من المكونات المترابطة (العتاد، البرمجيات) التي تسمح بجمع، معالجة، تخزين ونشر المعلومات من أجل المساعدة في تسيير العمليات، اتخاذ القرارات، التنسيق، المراقبة، التحليل وعرض الحالة الداخلية للمؤسسة وعلاقاتها مع الشركاء الخارجيين. (J.laudon, 2010, p. 07)
- مجموعة من الموارد البشرية، أدوات، إجراءات، البرامج، الي تقوم بجمع البيانات، معالجتها وتوزيعها على مختلف مستويات المؤسسة، بغرض تنفيذ الأعمال واتخاذ القرارات. (بلفكرات، 2019، صفحة 175)

من خلال التعريفين السابقين، نستنتج أن نظام المعلومات هو مجموعة من المكونات المترابطة والتي تتفاعل فيما بينها من أجل الوصول إلى نفس الهدف.

2- مكونات نظام معلومات المؤسسة:

تتكون نظم المعلومات المؤسسة من خمس موارد أساسية كما يلي: (بلفكرات، 2019، صفحة 178)

- ✓ **الموارد المادية:** وتشمل جميع الآلات من حواسب، شاشات طابعات، وحوامل التخزين وغيرها.
- ✓ **الموارد البشرية:** هناك حاجة ماسة للأفراد لتشغيل جميع أنظمة المعلومات، ويظم نظام المعلومات المؤسسة نوعين من الموارد البشرية:

- المتخصصين في نظام المعلومات: محللي النظام، المبرمجين والمشغلين.
- المستخدمين النهائيين: الأفراد الذين يستخدمون نظام المعلومات لاسترجاع المعلومات واستخدامها.

✓ **موارد البرمجيات:** هي المكونات التي تشمل النظم والبرمجيات الأساسية لتشغيل نظم المعلومات وتشمل نظم التشغيل، البرمجيات والتطبيقات.

✓ **موارد البيانات:** تتضمن جميع مكونات تكنولوجيا المعلومات اللازمة للمؤسسة، وتنظيم مورد البيانات في شكل قواعد بيانات، قواعد معرفة أو بنوك معلومات، التي توفر المعلومات لإعطاء خبرة في الميادين المختلفة.

✓ **مورد الشبكات:** تشكل الشبكات موردا هاما من موارد نظم المعلومات ومشاركتها، كما تتيح هذه الشبكات إمكانية استخدام برامج المساندة والوصول إلى قواعد البيانات المختلفة.

إضافة إلى المكونات المذكورة أعلاه، تجدر الإشارة إلى عنصر **الإجراءات**، التي يقصد بها السياسات والطرق التي يجب اتباعها عند استغلال وصيانة نظام المعلومات، حيث يجب اتباع هذه الإجراءات على سبيل المثال لتحديد وقت وعدد مرات تشغيل برنامج، ومن المخول لهم القيام بذلك، ومن لديه الحق في الوصول إلى التقارير النهائية. (devece, 2012, p. 15)

3- مخاطر أمن المعلومات في المؤسسة:

تعبر مخاطر أمن المعلومات عن تلك الأفعال والممارسات التي تهدف إلى إتلاف نظام معلومات المؤسسة كليا أو إلحاق الضرر به، حيث يمكن أن تقسم إلى التصنيفات التالية:

1.3 مخاطر مادية: هي تلك المخاطر المتعلقة بالأجهزة في حد ذاتها، والتي قد تكون سبب في تلفها الجزئي أو الكلي، كالسرقة وأعمال التخريب، نقص الصيانة والتحديثات، إضافة إلى التعطيلات والأخطاء في تصميم البرمجيات.

2.3 مخاطر بشرية (داخلية): ترتبط المخاطر البشرية غالبا بجهل وقلة وعي المستخدمين أكثر من رغبتهم في إلحاق الضرر بها من جهة، وعادة ما تنتج هذه المخاطر من الاستعمال الشخصي للأجهزة المعلوماتية المخصصة للعمل، وهذا ما يعرضهم إلى خطر الإصابة بالبرامج الخبيثة أو خطر تحميل البرامج

المقرصنة التي لا تكون متطابقة مع التطبيقات المعلوماتية المهنية، ومن جهة أخرى قد يكون الخطر الداخلي عن قصد ولعدة أسبابا تتمثل في (حديد، 2014، صفحة 190):

- **عدم الرضا:** جعلت التقنيات الحديثة مهاجمة نظم المعلومات أمرا يشعر بالانتقام للذات في نفس الشخص الذي ينفذ الهجوم.

- **إثبات الشخص مهاراته الفنية وقدراته على تنفيذ الهجوم الالكتروني:** هناك أشخاص يشعرون بالفخر عند تمكنهم من اختراق مواقع على شبكة الانترنت أو الوصول إلى قواعد بيانات محمية.

- **تحقيق المكاسب المالية:** قد يهاجم شخص ما أنظمة معلومات الجهة التي يعمل فيها لسرقة معلومات يستخدمها لاحقا بغرض الابتزاز لدفع فدية مالية.

3.3 مخاطر بيئية: يقصد بها تلك الحوادث الطبيعية التي يصعب على المؤسسة التحكم فيها أو مواجهتها، مثل الزلازل، الحرائق، الفيضانات والأعاصير.

4.3 مخاطر معلوماتية: تعتبر هذه التهديدات الأكثر انتشارا، وتتمثل في البرمجيات الخبيثة المختلفة التي تلحق أضرارا بليغة بمعلومات وأجهزة المؤسسة، وهذا ما دفع بالعديد من المؤسسات إلى الاختصاص في صناعة وسائل الحماية، ومن بين الطرق التي تسمح بانتقال هذه البرمجيات نذكر استعمال وسائط التخزين، الرسائل أو الروابط المشبوهة عبر البريد الالكتروني، تصفح المواقع المشبوهة التي تستغل الثغرات الأمنية على جهاز المستخدم، تحميل برامج من الأنترنت التي يمكن أن تحتوي على برامج خبيثة. (حديد، 2014، الصفحات 189-190)

4- أشكال الاعتداءات المعلوماتية على نظام معلومات المؤسسة

نتيجة لتطور تكنولوجيا المعلومات والاتصالات تطورت أساليب وأشكال الاعتداءات على أجهزة، برامج وشبكات المؤسسة، واستغلال أي ثغرة بنظام معلوماتها من أجل اختراقها وإلحاق الضرر بها، ومن بين هذه الاعتداءات نذكر:

1.4الاعتداء باستعمال البرامج الخبيثة: تستخدم البرامج الخبيثة في تعطيل عمل الحاسبات وإلحاق الضرر بالشبكات وتدمير المواقع الالكترونية وسرقة المعلومات وغيرها من الأعمال غير المشروعة، وتشمل أنواعا عديدة يمكن تلخيصها فيما يلي:

- **حصان طروادة Trojan Horse** :برنامج يتضمن إجراءات خفية يعرفها المعتدي وحده تسمح له بإتلاف انظمة الحماية، يقوم بفتح منفذ « باب خلفي» بنظام استغلال الجهاز المصاب والقيام بالوظائف المبرمجة من قبل المعتدي. (مسوس، 2016، صفحة 33)
- **القنبلة المنطقية Logic bomb** :برنامج خبيث بسيط قادر على إلحاق الضرر بالحواسيب بطريقة ساكنة، أي تنفذ إجراءاتها عند وقوع حدث معين فقط مثلا: تاريخ معين، فعل معين أو إدخال بيانات معينة كسلسلة حروف معينة. (بوزيد سمية، 2018، صفحة 74)
- **الفيروس المعلوماتي Virus** :تم استعمال لفظ فيروس معلوماتي لأول مرة سنة 1986، هو عبارة عن برنامج معلوماتي يتضمن أهداف تدميرية للأجهزة المصابة ولكل محتوياتها، وتتميز بقدرتها على نسخ نفسها في البرنامج الذي تصيبه، والتحكم به وتعديله، وبقدرته على الانتقال من برنامج لأخر بداخل بنفس الجهاز. (حديد، 2014، صفحة 191)
- **الدودة المعلوماتية Worm:** فيروس معلوماتي يمتاز بقدرته على التنقل عبر الشبكات. (wolfhugel, 2007, p. 56)
- **الفدية المعلوماتية Ransonware**: برنامج يصيب الحواسيب والأجهزة المحمولة، يعمل على تشفير بيانات هذه الأجهزة أو التحكم بها كليا ومنع المستخدم من الوصول إليها إلا بعد دفع مبلغ مالي كفدية مقابل فك التشفير عن ملفاته.

هذه الفدية لا تكون في شكل عملة فيزيائية، بل عملة رقمية مشفرة، أهمها عملة **'Bitcoin'** وتعد العملة الرقمية الأكثر تداولا في مواقع الأنترنت وتستخدم لجعل التعاملات المالية افتراضية.)بوزيد سمية, 2018(76 .p ,)

2.4 الاعتداء باستعمال برامج الجوسسة

هي عملية استغلال المعلومات بطريقة غير مشروعة من خلال تثبيت برنامج جوسسة داخل النظام، حيث يتواصل مع وكيل خارجي عن طريق ما يعرف بالباب الخلفي، (wolfhugel، 2007، صفحة 57)نذكر منها:

- **مسجل نقرات لوحة المفاتيح Keylogger**: هاز أو برنامج يقوم بتخزين كل البيانات التي يكتبها المستخدم على لوحة مفاتيح حاسوبه ثم يرسلها إلى المعتدي عبر الأنترنيت، لمعرفة كلمات السر، أرقام البطاقات البنكية وغيرها من البيانات الحساسة. (بوزيد سمية، 2018، صفحة 78)
- **ملف تعريف الارتباط Cookies**: لف نصي صغير يحتوي على معلومات يمكن من خلالها تسيير، تخزين ورصد زيارات المتصفح للمواقع الإلكترونية، يكمن خطر هذه الآلية في إمكانية استعمالها كأداة للمراقبة، كونها تجمع وتحليل المعلومات لمعرفة عادات، خيارات وأذواق المتصفح. (حديد، 2014، صفحة 192)
- **برنامج اعتراض البيانات Sniffing**:اعتراض البيانات هو تقنية تسمح باستراق السمع للبيانات التي يتم تبادلها عبر الشبكات، أي بعد إرسالها وقبل استقبالها، وتحليلها بغرض الاستفادة منها بصورة غير شرعية. ويستخدم لهذا الغرض برمجيات تدعى 'Sniffers' التي تستخدم في مجالات عديدة في إطار التجسس عبر الشبكات. (بوزيد سمية، 2018، صفحة 79)
- **البرامج الإعلانية Adware**:على غرار البرامج الخبيثة، تكون برامج الجوسسة محتواة في برامج إعلانية تعرف باسم Adware، التي تعمل على إظهار نوافذ إشهارية غير مرغوب فيها. (مسوس، 2016، صفحة 34)

3.4 الاعتداء باستعمال أسلوب انتحال عنوان IP*: المقصود بهذا الأسلوب تخفي المعتدي، من خلال انتحال صفة مستخدم آخر عن طريق تزوير عنوان **IP** الخاص به، وهذا ما يسمح له بإخفاء كل أثر يؤدي إلى التعرف عليه في حالة اكتشاف الاعتداء.

5.4 الاعتداء باستعمال أسلوب انتحال عنوان DNS**: المقصود بهذا الأسلوب توجيه مستخدمي الانترنت اوتوماتيكيا إلى المواقع المحتوية على برامج جوسسة أو المواقع التي تحاكي في تصميمها المواقع التجارية والبنكية والتي تصمم من قبل المعتدين بغرض الإيقاع بهم. (بوزيد سمية، 2018، صفحة 80)

* IP: Internet Protocol

6.4 الاعتداء باستعمال أسلوب منع تقديم الخدمة DDOS* :الحرمان من الخدمة الموزعة، هو ذلك الهجوم الذي يهدف إلى إيقاف قدرة الخادم على تقديم الخدمات المعتادة أو المفترض تقديمها، وذلك عن طريق إغراقه بكم كبير من الإيعازات تؤدي لتوقفه عن العمل أو الحد عن قدرته على العمل بصورة طبيعية، باستخدام برمجيات تدعى **Flooders**.

يتم من خلال هذه التقنية استخدام عدة أجهزة متصلة فيما بينها على الأنترنيت تسمى شبكات **'Zombies'** والي يتحكم فيها عن بعد ودون علم أصحابها.

7.4 الاعتداء باستعمال أسلوب البريد غير المرغوب: تعرف رسائل البريد الالكتروني غير المرغوب بأنها إساءة استخدام نظام الرسائل الالكترونية من خلال إرسال كم هائل من الرسائل العشوائية غير المطلوبة أو المتوقعة او المرغوبة من قبل المستقبلين لهذه الرسائل، وغالبا ما يكون الغرض من هذه الرسائل هو الإعلان التجاري أو الاحتيال على صاحب البريد الالكتروني. (حديد، 2014، صفحة 193)

8.4.الاعتداء باستعمال أسلوب الهندسة الاجتماعية: منهجية لا تعتمد على الوسائل التقنية بل هي أسلوب اختراق يعتمد على العنصر البشري من خلال التلاعب بالأفراد وخداعهم بحيل نفسية لكسر الإجراءات الأمنية والوصول غير المشروع إلى أنظمة الحاسوب.

تعد الهندسة الاجتماعية من الأساليب سهلة التنفيذ مقارنة بالوسائل الأخرى لكنها لا تقل عنها أهمية، فهي جد فعالة للحصول على المعلومات من الأفراد المستخدمين للأنظمة الذين يُعتبرون الحلقة الأضعف للأمن الإلكتروني في حال جهلهم وقلة وعيهم وتكوينهم في هذا المجال. (بوزيد سمية، 2018، صفحة 80)

5- أمن نظم معلومات المؤسسة

تستخدم المؤسسة العديد من الوسائل التقنية والتنظيمية، قصد محاولة حماية نظم معلوماتها أو التقليل من أضرار مختلف المخاطر والاعتداءات التي تتعرض لها، حيث يعتبر أمن نظم المعلومات من بين الركائز الأساسية التي تأخذها بعين الاعتبار.

** DNS: Domain Name System
* DDOS : Distributed Denil Of Service

1.5.تعريف الأمن المعلوماتي: هو تلك الممارسات التي تهدف إلى حماية الانظمة، الشبكات والبرامج من الاعتداءات المعلوماتية سواء كانت من داخل او خارج المؤسسة (IBM، 2022)، والتي تهدف عادة إلى الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على أموال أو اعتراض الأعمال الالكترونية. (Cisco, 2022)

كما يعرف على أنه مجموعة من المناهج والتقنيات والادوات التي تسمح بحماية موارد نظام المعلومات بالمؤسسة من اجل توافر المعلومات، سريتها وسلامة محتواها.

من خلال ما سبق، نستنتج أن أمن نظام المعلومات يهدف إلى:

- منع انتشار المعلومات بطريقة غير شرعية.
- منع تغيير المعلومات وتعديلها بطريقة غير مرخصة.
- منع الاستعمال غير المرخص للموارد المعلوماتية والشبكات. (حديد، 2014، صفحة 197)

2.5. ركائز أمن نظام المعلومات المؤسسة: من أجل حماية نظم المعلومات من المخاطر التي تتعرض لها لا بد من الأخذ بعين الاعتبار توفر مجموعة من الركائز للوصول إلى تحقيق الحماية اللازمة للمعلومات، وتتمثل هذه الركائز فيما يعرف بثلاثية CIA، وهي: (بوزيد سمية، 2018، صفحة 86)

– **السرية** confidentiality: وتعني حناية المعلومة من الإفشاء، أي ضمان أن الاطلاع عليها ونشرها لا يحق إلا للأشخاص المسموح لهم بذلك، والمقصود بالاطلاع على المعلومة قراءتها وطباعتها أو مجرد العلم بها.

– **السلامة** integrity: وتعني حماية المعلومة من الإفساد، أي ضمان صحة ودقة المعلومة ومنع تغيير شكلها ومحوها وتعديلها أو حتى إضافة معلومة جديدة بصورة عمدية أو عرضية إلا للأشخاص المسموح لهم بذلك.

– **التوافر** availibility: يعني حماية المعلومة من الانقطاع، أي ضمان استمرارية الوصول أو النفاذ إلى المعلومة في الوقت المناسب من طرف الأشخاص المسموح لهم بذلك، والوقاية من التوقف المفاجئ في وظائف نظام المعلومات.

إضافة إلى العناصر السابقة، تم إضافة عنصرين هما: (مسوس، 2016، صفحة 36)

–**الموثوقية** authentification: وتعني التحقق من هوية المستخدم، أي أن الشخص أو الجهة المتعامل معها هي ذاتها دون أي لبس او غموض.

–عدم الإنكار: القدرة على ضمان عدم إنكار الطرف المتعامل معه لوقوع المعاملة والنتائج المترتب عنها، فهي تتعلق بمسؤولية الشخص اتجاه الفعل الذي قد يكون إرسال رسالة أو أي فعل آخر.

3.5. الوسائل التقنية لحماية نظام معلومات المؤسسة: يعد تنفيذ تدابير الأمن المعلوماتي بشكل فعال أمرا صعبا، خاصة في البيئة الحالية التي تتميز بوجود الأجهزة أكثر من المستخدمين وأشكال الاعتداءات أكثر ابتكارا، الأمر الذي يفرض على المؤسسة استخدام مختلف الوسائل التقنية للوقاية من المخاطر المعلوماتية أو التخفيف من حجم الضرر الناتج عنها، وفيما يلي نستعرض مجموعة من هذه الوسائل.

– كلمة المرور:Pass Word في الواقع، أول عنصر يبحث عنه المعتدون هو محاولة الحصول على كلمات المرور، وخاصة تلك التي تكون ضعيفة أو سهلة الكشف، وكلمة المرور بكل أنواعها التي تسمح بالولوج إلى أنظمة الاستغلال أو التطبيقات أو الملفات هي إحدى أقدم الطرق وأبسطها للتحكم في النفاذ إلى الأنظمة والوصول إلى المعلومات، حيث ينبغي اختيارها اختيارا جيدا بحيث لا تكون سهلة التخمين والكشف وهذا عبر المحافظة عليها، ومن بين الإرشادات الواجب العمل بها لأجل هذا نذكر:

- التغيير الدوري لكلمة المرور.
- التزام الحد الأدنى لطول كلمة المرور .
- مزج الحروف الكبيرة والصغيرة مع الأرقام والرموز لتشكيل كلمة المرور .
- عدم ارتباط كلمة المرور بأي معلومات شخصية عن المستخدم. (بوزيد سمية، 2018، الصفحات 101-102)

– البرامج المضادة للبرامج الخبيثة Anti Malware : هي برمجيات تسمح بحماية نظام المعلومات من مختلف المخاطر والاعتداءات المعلوماتية (الفيروسات، برامج التجسس...)، يمكن تثبيت هذه البرمجيات على الحاسب الشخصي، الخادم أو حتى على الشبكات والفضاء السحابي. (lebigdata.fr، 2022)

تتضمن البرامج المضادة للبرامج الخبيثة قاعدة بيانات تمكنها من تحديد والتعرف على مختلف البرنامج الخبيثة قصد تعطيلها وإبطال مفعولها، ومن أجل فعالية مثلى لها يجب تحديثها وتحيينها باستمرار.

– الجدران النارية Firewall : هي مجموعة من البرمجيات والأجهزة المادية التي تعمل على صد كل دخول غير مرخص لنظام المعلومات من خلال تشكيل حدود فاصلة بين الشبكة الداخلية للمؤسسة

والأنترنت، كما يقوم بدور المرشح لمراقبة كل التدفقات التي تمر عبره دخولا وخروجا. (J.laudon, 2010, p. 81)

– **التشفير Cryptography** : عبارة عن عملية رياضية –معادلات خوارزمية– يتم من خلالها تحويل النص المراد إرساله إلى رموز وإشارات لا يمكن فهمها إلا بعد القيام بفك الشيفرة وتحويل الرموز والإشارات إلى نص مقروء من خلال استخدام مفاتيح التشفير، هذه العملية لا تتم إلا إذا كان الطرف الآخر يمتلك مفتاح فك الشيفرة الذي يحول تلك الإشارات والرموز إلى النص الأصلي، (مسوس، 2016، صفحة 36) وينقسم التشفير إلى نوعين:

- التشفير المتماثل: يستخدم فيه نفس المفتاح للتشفير وفك الشيفرة.
- التشفير غير المتماثل: يستخدم فيه مفتاحان لكل مستخدم، أحدهما عام للتشفير والآخر خاص لفك الشيفرة.

– **أسلوب الشبكة الخاصة الافتراضية VPN*:** هو أسلوب قائم على إنشاء ممر خاص وامن بين طرفي المرسل والمستقبل يتم من خلاله تبادل رسائل مشفرة، يعتمد على بروتوكول IPsec.

– **أسلوب الأمن من خلال بروتوكول SSL**:** يسمح بتشفير كل بيانات المعاملات بين المؤسسة والمتصلين بها عبر الأنترنت، حيث يوفر هذا الأسلوب إمكانية التأكد من موثوقية الموقع وعدم تزييفه، من خلال الشهادة الالكترونية المتحصل عليها.

– **الشهادة الالكترونية:** هي وثيقة تمنحها الهيئات المتخصصة في أمن المعلومات، تستخدم لتحقيق سرية المعاملات من خلال إجراء عمليات التشفير المطلوبة وكذا التأكد شخصية الطرفين المتعاملين وضمان عدم كشف بيانات كليهما. (27001:2013(fr), 2022)

– **التوقيع الالكتروني:** يعرف كذلك بالبصمة الالكترونية، هو أسلوب يتم من خلاله التأكد من هوية القائم بالمعاملة.

يجدر التنويه أن أمن نظم المعلومات لا يقتصر على الوسائل التقنية المذكورة أعلاه، حيث أن للعنصر البشري دورا لا يقل أهمية في تعزيزه، كونه القائم على سير الإجراءات التنظيمية والعملية، من

* VPN : Vertual Private Network
** SSL : Secure Socket Layer

خلال مسؤولياته، الأمر الذي يستوجب نشر الوعي وتدريب المستخدمين على أمن نظم المعلومات لتجنب الخسائر المادية والمعنوية (السمعة).

6- مجالات الأمن المعلوماتي في المؤسسات الجزائرية: وضعت وزارة البريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة الجزائرية، مرجعية وطنية لحماية المعلومة (RNSI[***])، تحت تصرف المؤسسات والهيئات العمومية، تصر إصدارها سنة 2020 وهي نسخة معدلة للنسخة الأولى الصادرة سنة 2016، عن نفس الهيئة.

تهدف المرجعية الوطنية لأمن المعلومة (RNSI 2020) إلى توفير التدابير والإجراءات الأساسية من أجل تطوير وتحقيق أمن نظم المعلومات داخل المؤسسات والهيئات العمومية والإشراف عليها، إضافة إلى تقديم توصيات حول حماية المعلومات وإدارة المخاطر المتعلقة بسريتها، سلامتها وتوافرها، وهذا من خلال مجموعة من الإجراءات:

- وضع ضوابط أمنية مناسبة للرفع من مستوى أمن نظم المعلومات وأمن المعلومة.
- تبني مقاربة ترتكز على تقييم المخاطر عند تطبيق الرقابة الأمنية.
- تحديد الأدوار والمسؤوليات المتعلقة بحماية المعلومة.

تم وضع مجموعة من الإجراءات والضوابط بهذه المرجعية، لتلبية الاحتياجات من جانب الأمن المعلوماتي لجميع الهيئات والمؤسسات التي تنشط على المستوى الوطني مع مراعات خصائص كل قطاع والأخذ بعين الاعتبار النظام الداخلي، طبيعة النشاط، التقنيات المستعملة والتركيز على وجود إدارة للمخاطر المتعلقة بأمن نظام المعلومات، إضافة لمراقبة وتقييم دوريين للإجراءات الأمنية.

تضمنت المرجعية الوطنية لأمن المعلومة (RNSI 2020)، قائمة بعشرين (20) مجال لأمن المعلومة "أنظر الملحق رقم 1"، نلخصها كما يلي:

- ✓ إدارة الأصول: كل الأصول المتعلقة بنظام المعلومات وتحديد المسؤوليات المنصوص عليها من أجل أمن المعلومة.
- ✓ حماية البيانات الشخصية: المتعلقة بالمستخدمين أو المواطنين.

*** RNSI : Référentiel National de Sécurité de l'Information

- ✓ إدارة ومراقبة تراخيص الدخول: السماح للأشخاص المخول لهم فقط الوصول إلى المعلومة.
- ✓ أمن الأجهزة المحمولة: على غرار تراخيص الدخول أو الحماية من البرامج الخبيثة.
- ✓ حماية المعلومات على الشبكات.
- ✓ أمن نظم المعلومات: تحديد المتطلبات الأمنية لنظم المعلومات وضمان تطبيقها طول دورة حياة النظام.
- ✓ الأمن المرتبط بالاستغلال: ضمان التشغيل الصحيح والآمن للوسائل.
- ✓ أمن نظم المعلومات الحرجة: التأكد من تنفيذ جميع الإجراءات.
- ✓ أمن الخدمات السحابية: أمن المعلومات المخزنة، المعالجة والمسترجعة عبر الخدمات السحابية.
- ✓ التشفير: التأكد من سرية وسلامة المعلومات الحساسة من خلال تنفيذ تدابير التشفير المناسبة، بما يتماشى مع السياسات والإجراءات الأمنية للمؤسسة، وكذلك القوانين المعمول بها (الجزائرية الدولية).
- ✓ الأمن المادي: حماية المستخدمين، المعلومات، المعدات والبنى التحتية للمؤسسة من كل المخاطر.
- ✓ أنترنت الأشياء: العمل على وجود مجموعة من الضوابط لأنترنت الأشياء عند استعمالها من طرف المؤسسة.
- ✓ المراقبة والتسجيل: تسجل نشاطات المستخدمين، الاستثناءات، الاختلالات والأحداث المتعلقة بأمن المعلومات، البحث عن الأدلة وكشف الحوادث الأمنية.
- ✓ إدارة السوابق الأمنية: التأكد من معالجة كل الثغرات الأمنية ونقاط الضعف التي تم الإبلاغ عنها مع وضع ضوابط لتجنب تكرارها.
- ✓ إدارة استمرارية العمل: ضمان استمرارية نشاط وعمل نظم المعلومات خاصة الحساسة منها والعمل على الحد من تأثير المخاطر على الأشخاص، العمليات، والبنى التحتية.
- ✓ الموارد البشرية: توعيتهم بتهديدات الامن المعلوماتي ودورهم في تحقيق أمن المعلومات قبل، أثناء وبعد عقد العمل.

- ✓ الأمن المتعلق باستخدام شبكات التواصل الاجتماعي: يجب على المؤسسات التي تستخدم شبكات التواصل الاجتماعي ضمن نشاطها، وضع تدابير أمنية على جميع المستويات.
- ✓ ضمان إدراج الأمن خلال جميع مراحل تطوير البرمجيات: التأكد من أن أمن المعلومات جزء لا يتجزأ من امن نظام المعلومات طوال دورة حياته، إضافة لتطوير الإجراءات الامنية باستمرار.
- ✓ المتطلبات الأمنية لمشاريع تكنولوجيا المعلومات: مراعاة شروط أمن المعلومات خلال دورة حياة المشروع وفقا للسياسات الأمنية، المتطلبات التنظيمية والتشريعية.
- ✓ العلاقة مع الشركاء مقدمو الخدمات: التأكد من وجود إجراءات أمنية خلال فترة استفادة المؤسسة من خدمات باستعانتها بأطراف أخرى، أي أنها لا تشكل أي تهديدات.

تجدر الإشارة أن المرجعية الوطنية لأمن المعلومة (RNSI 2020) تتضمن كذلك نموذج ميثاق (Charte) الأمن المعلوماتي، الذي يساعد المؤسسات الجزائرية في صياغة ميثاق داخلي خاص بها، يسهل على المستخدمين فهم إجراءات أمن نظام المعلومات والتقيد بها.

7.معايير أمن نظم معلومات المؤسسة:

من أجل ضمان أمن نظام المعلومات، يمكن للمؤسسة الاعتماد على مجموعة من المعايير والمرجعيات، نذكر أهمها:

1.7. معيار ISO-IEC 27001:هو المعيار الدولي لأمن نظم المعلومات الاكثر انتشارا، تم نشره من طرف المنظمة الدولية للتقييس ISO واللجنة الالكتروتقنية الدولية IEC، سنة 2005، تحدد هذه المعايير نظام يومي ومتطلبات إنشاء، تنفيذ، تحيين، والتحسين المستمر لنظام إدارة أمن المعلومات بالمؤسسة، حيث تمنح شهادات معتمدة للمؤسسات التي تلتزم بالشروط التي تنص عليها المنظمة.

2.7.معيار ISO-IEC 27002:هو دليل الممارسات الجيدة لإدارة أمن المعلومات، يوفر إرشادات حول التدابير التنظيمية والممارسات السليمة لإدارة أمن المعلومات والتي تشمل أمن الموارد البشرية، الموارد المادية، البرمجيات والشبكات، دون إمكانية تقديم شهادات. (مسوس، 2016، الصفحات 42-43)

3.7. طريقة MEHARI: تعمل هذه الطريقة على تحقيق الأمن المعلوماتي بالمؤسسات من خلال تحليل المخاطر المعلوماتية مع تحديد الموارد، الوسائل والإجراءات اللازمة لتنفيذها، وهذا وفق المراحل الثلاث التالية: (مسوس، 2016، صفحة 43)

-تحليل وتقييم المخاطر: تتضمن التحليل المنهجي والآلي للحالات التي تنطوي على مخاطر وتحليل المخاطر في المشاريع الجديدة.

- تشخيص حالات السلامة المعلوماتية: تتضمن تشخيص السلامة المعلوماتية كعنصر من عناصر تليل المخاطر، المخططات الامنية على أساس التشخيص، الدعم المقدم من قواعد المعرفة لإنشاء إطار مرجعي للسلامة المعلوماتية، المجالات التي تشملها وحدة التشخيص الامني.

- تحليل الرهانات: تتضمن تحليل الرهانات الأمنية كأساس لتحليل المخاطر وتصنيف الأصول كعنصر أساسي لسياسة السلامة المعلوماتية، إضافة إلى تحليل الرهانات الأمنية كأساس للتخطيط الأمني، ونظرة عامة حول استخدام منهجية MEHARI.

4.7. مرجعية COBIT: طريقة وضعتها جمعية تدقيق ومراقبة نظام المعلومات **ISACA**[***] سنة 1996، تهدف هذه المرجعية إلى مساعدة المؤسسات على التحكم ومراجعة نظم المعلومات وكذا إدارة المخاطر المتعلقة بهذه الأخيرة، تتناول مرجعية **COBIT** من جانب حوكمة أمن المعلومات العناصر التالية:

- الأخذ بعين الاعتبار أمن المعلومات داخل الاصطفاف الاستراتيجي.
- اتخاذ مختلف التدابير المناسبة للحد من المخاطر والاعتداءات الالكترونية إلى حد مقبول.
- المعرفة أو ما يسمى حاليا باليقظة الامنية، وحماية الأصول.
- إدارة الموارد بطريقة تضمن أمن الانظمة المعلوماتية.
- القياس من أجل ضمان تحقيق الأهداف الأمنية.
- خلق القيمة من خلال تحسين الاستثمارات في مجال أمن المعلومات.
- دمج أمن المعلومات داخل سيرورة المؤسسة.

8- إجراءات أمن نظام المعلومات على مستوى مؤسسة الإنجازات الكهربائية REELEC:

[***] ISACA : The Information Systems Audit And Control Association

1.8.التعريف بالمؤسسة محل الدراسة: رييلاك مؤسسة عمومية اقتصادية متخصصة في تصميم وإنجاز التركيبات الكهربائية الصناعية، كما تضمن صيانة التجهيزات الكهربائية ذات الضغط المنخفض والمتوسط والعالي، بما في ذلك المولّدات الكهربائية، وقد اكتسبت خبرة مؤكدة في إعداد الدراسات وتركيب لوحات التوزيع الكهربائية، مع تقديم حلول متكاملة لتحقيق فعالية طاقوية مثلى.

2.8.محور نشاط المؤسسة محل الدراسة: حاليًا، يتمحور نشاط رييلاك بشكل أساسي على قطاعات استراتيجية متنوعة، لها عوامل نجاح مشتركة، على إثرها تم تحديد النشاطات الاستراتيجية، التالية:

- الدراسات والهندسة في مجال الكهرباء الصناعية بما في ذلك الفحص والتشخيص الطاقوي وتعويض الطاقة الارتكاسية.
- صيانة المنشآت الكهربائية ومختلف محطات المحولات الكهربائية 10، 30، 60، 220 كيلو فولت.
- شبكات التوزيع الكهربائي (الضغط العالي، المتوسط والمنخفض).
- تركيب نظام المراقبة والتحكم الرقمي.
- تركيب وصيانة المولدات الكهربائية.
- وضع أنظمة الحماية المضادة للبرق.
- إضاءة المطارات. (https://WWW.REELEC.DZ، 2022)

فيما يتعلق بتسيير المشاريع، استفادت رييلاك من تجربة قوية استمرت لأكثر من نصف قرن، كسبت من خلالها مهارات متميزة، مما جعلها رائدة بين منافسيها في سوق المؤسسات الكبرى، مثل سوناطراك، شركة الكهرباء والغاز، نفطال...

في إطار التحول الطاقوي، ومن أجل فعالية طاقوية أفضل، وضعت رييلاك استراتيجيات متنوعة في مجال الطاقة الكهربائية النظيفة، من خلال تقديم حلول متكاملة تعتمد على الطاقة الكهروضوئية، انطلاقا من الخدمات الهندسية إلى توريد الأجهزة والأشغال المتعلقة بتركيب الألواح الشمسية وأجهزة التزويد المستمر للطاقة.

إن الفعالية، الأداء، والمهنية تعتبر من القيم الأساسية للفريق المشكّل لمؤسسة ريبلاك، ممّا منحها مكانة رائدة في سوق تركيب الأجهزة الكهربائية.

تقع المؤسسة مل الدراسة بنهج محمد قاسي – ص ب 08- بابا حسن، 16081 الجزائر العاصمة، الجزائر.

3.8 إجراءات أمن نظام المعلومات على مستوى المؤسسة محل الدراسة: تعتمد مؤسسة الإنجازات الكهربائية EPE REELEC SPA، مجموعة من الإجراءات والتدابير لأمن نظام معلوماتها، والتي يعمل على تنفيذها وتطويرها قسم نظام المعلومات بالمؤسسة ونذكر منها:

– **كلمة المرور:** إلزامية توفر كلمة المرور على كل أجهزة الكمبيوتر، كما يتم تغييرها بشكل دوري كل ثلاثة 03 أشهر، حيث يستقبل المستخدم رسائل ترسل آليا من طرف قسم نظام المعلومات بهدف التذكير بضرورة تغيير كلمة المرور.

– **البرمجيات المضادة للبرامج الخبيثة:** تعتمد المؤسسة على برمجية **Kaspersky administration kit**، الذي يتم تفعيله مباشرة بالخادم (serveur) الرئيسي، والذي بدوره يضمن الحماية لكل الأجهزة، البرمجيات والشبكات المتصلة به.

– **جدار النار:** تستعمل المؤسسة نوعين من جدران النار: أحدهما من إنتاج شركة مايكروسوفت، خاص بالخادم الرئيسي، لترشيح التدفقات بينه وبين الأجهزة المتصلة به، أما جدار النار الثاني، هو عبارة عن برمجية (**PF SENSE**)، المفتوحة (**OPEN SOURCE**)، يتم تفعيها وتهيئتها عبر الانترنت.

– **بروتوكول SSL**: تمتلك المؤسسة شهادة **SSL** لإنشاء حماية بين خادم الويب والمتصفح لمن خلال موثوقية موقعها الالكتروني وعدم تزييفه.

– **خدمة DNS**: تستخدم المؤسسة هذه التقنية لحجب بعض المواقع حتى لا يتمكن المستخدمين تصفها والوصول إليها، على غرار مواقع التواصل الاجتماعي.

قامت المؤسسة بوضع ميثاق داخلي للأمن المعلوماتي (charte de sécurité informatique)، تم وضعه تحت تصرف المستخدمين على الشبكة الداخلية للمؤسسة، قصد الاطلاع عليه والتقيد ببنوده المتضمنة إجراءات الأمن المعلوماتي والالتزام بها، إضافة إلى تزويد الوافدين الجدد إلى المؤسسة بنسخة منه مرفق بالنظام الداخلي للمؤسسة لتحسيسهم وتوعيتهم بأهمية الأمن المعلوماتي. (https://WWW.REELEC.DZ، 2022)

9. نتائج الدراسة

1) تواجه المؤسسة مجموعة من المخاطر (المادية، البشرية، البيئية والمعلوماتية)، والتي تهدد أمن نظام معلوماتها.

2) تتعدد وتتنوع أشكال الاعتداءات المعلوماتية على نظام معلومات المؤسسة، حيث أصبحت أكثر تطورا وابتكارا وهذا نتيجة لتطور تكنولوجيا المعلومات والاتصال.

3) تعتمد المؤسسة على مجموعة من الممارسات، التقنيات والأدوات لحماية نظام معلوماتها وضمان توافر المعلومات، سريتها وسلامة محتواها.

4) وضعت وزارة البريد والمواصلات السلكية واللاسلكية والتكنولوجيا والرقمنة الجزائرية مرجعية وطنية لحماية المعلومات (RNSI 2020)، تحت تصرف المؤسسات والهيئات العمومية، من أجل تطوير وتحقيق أمن نظم المعلومات.

5) يوجد مجموعة من المرجعيات والمعايير الدولية لأمن نظم المعلومات على غرار ISO-IEC 27001، وهو المعيار الأكثر انتشارا.

6) تعتمد مؤسسة الإنجازات الكهربائية EPE REELEC SPA، على مجموعة من الإجراءات والتدابير لضمان أمن نظم معلوماتها.

7) نظم المعلومات لا يقتصر على حماية الأفراد والأجهزة فقط، بل يوجد مجموعة من البرامج الخبيثة المتنقلة عبر الشبكات، وتشكل تهديدا حقيقيا لأمن المعلومات.

8) تكوين ثقافة الأمن المعلوماتي من خلال تكوين الأفراد ونشر الوعي بين الأطراف المعنية للمؤسسة حول ضرورة وأهمية أمن نظم المعلومات، لضمان سرية، سلامة وتوافر المعلومة.

9) العمل على تطوير وتحيين الإجراءات، التقنيات والتدابير الخاصة بأمن نظم معلومات المؤسسة بشكل دائم ومستمر، وفق المتطلبات الجديدة التي تمليها طبيعة المخاطر والاعتداءات المعلوماتية المستحدثة والمتنامية والتي أصبحت أكثر تطورا وابتكارا وأشد انتشارا.

10.خاتمة:

شهد نظام معلومات المؤسسة عدة تطورات تقنية، برمجية وعلى مستوى الشبكات، نتيجة لتطور تكنولوجيا المعلومات والاتصال، كما رافق هذه التطورات عدة مخاطر مبتكرة تهدد أمن نظام المعلومات، أصبح من السهل اختراق أي نظام معلومات لا يتوفر على الإجراءات الأمنية اللازمة لحمايته، وعليه وضعت وزارة البريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة تحت تصرف المؤسسات الجزائرية مرجعية وطنية لأمن المعلومة، إضافة لوجود عدة معايير ومرجعيات دولية اهتمت بهذا الموضوع لحساسيته وأهميته البالغة.

11. قائمة المراجع:

1) بلفكرات رشيد(2019) ، دور نظم المعلومات الإدارية في اتخاذ القرار الإداري .مجلة الحقوق والعلوم الانسانية دراسات اقتصادية، العدد 37.
2) بوزيد هجيرة سمية، (2018) ،الأمن الالكتروني كضرورة لنجاح مشروع الحكومة الالكترونية– حالة الجزائر .أطروحة دكتوراه ،علوم تسيير، جامعة الجزائر 3.
3) حديد نوفل، كريبط حسان .(2014) ،أمن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة .مجلة المؤسسة، العدد 3،جامعة الجزائر 3.
4) مسوس كمال, حديد نوفل، (2016) ،مقاربات حماية أنظمة معلومات المؤسسة من الاعتداءات الالكترونية .مجلة المؤسسة ، جامعة الجزائر 3، العدد 5.
5) J.laudon, K. &. (2010). management des systèmes d'information. france: person éducation.
6) devece, R. l. (2012). introduction to management information systems. france: Jaume university.
7) wolfhugel, 1. L. (2007). securite informatique principes et methode. parise, france, france: edition eyrolles.
8) https://www.ibm.com/topics/cybersecurity, consulté le 31/08/2022.
9) https://www.cisco.com/c/en/us/pruducts/security/what-is-cybersecurity.html, consulté le 31/08/2022.
10) https://www.lebigdata.fr/antimalware-definition, consulté le 31/08/2022.
11) https://www.iso.org/obp/ui/iso:std:iso-iec:27001:ed-2:v1:fr, consulté le 31/08/2022.

12)https://WWW.REELEC.DZ . (2022, 12 20).

12.ملاحق:

ملحق رقم 1: قائمة عشرين (20) مجال لأمن المعلومة المنصوص عليها لمرجعية الوطنية لأمن المعلومة RNSI 2020)(

Codification des domaines :

Code du domaine		Domaines (Français)	Domains (Anglais)
1	AM	Gestion des actifs	Asset Management
2	PDP	Protection des données à caractère personnel.	Personal Data Protection.
3	ACM	Gestion et contrôle des accès.	Access Control Management
4	MDS	Sécurité des appareils mobiles	Mobile Devices Security
5	NTSEC	Sécurité des réseaux	Network Security
6	SYSEC	Sécurité des systèmes d'information	System Security
7	OPSEC	Sécurité liée à l'exploitation	Operation Security Controls
8	SCS	Sécurité des Système d'information critiques	Security of Critical Systems
9	CLDSEC	Sécurité des services cloud	Cloud Security
10	CRYPT	Cryptographie.	Cryptography
11	PHYSEC	Sécurité Physique	Physical Security
12	SECIOT	Internet des Objets	Internet Of Things (IoT)
13	LMO	Surveillance et Journalisation	Loggings and Monotoring
14	SECIM	Gestion des Incidents de sécurité	Security Incident Management
15	BCM	Gestion de la continuité des activités	Business Continuity Management
16	SECRH	Ressources humaines	Human Resources
17	SMSEC	Sécurité liée à l'usage des Réseaux Sociaux	Social Media Security
18	SSDLC	Intégration de la sécurité durant le cycle de vie de développement des logiciels	Secure Software Development life cycle (SSDLC)
19	SECPRJ	Exigences de Sécurité pour les projets de technologie de l'information	Security Requirements for IT Projects.
20	CTP	Relation avec les tierces parties.	Contact with Third Parties