

واقع إدارة أمن المعلومات في مؤسسة السويدي إلكترونيك الجزائرية. *The reality of information security management in the "Elsewedy Electric Algeria".*

—هاجر بوعوة /مخبر إدارة التغيير في المؤسسة الجزائرية جامعة الجزائر3، طالبة دكتوراه، bouaoua.hadjer@univ-alger3.dz

—أمال موترفي /مخبر إدارة التغيير في المؤسسة الجزائرية جامعة الجزائر3، أستاذة محاضرة أ، mouterfi.amel@univ-alger3.dz

تاريخ النشر: 2020/01/23

تاريخ القبول: 2020/01/08

تاريخ الإرسال: 2019/10/27

ملخص

تهدف هذه الدراسة إلى معرفة واقع إدارة أمن المعلومات في مؤسسة "السويدي إلكترونيك الجزائرية" من خلال محاولة إبراز مختلف التقنيات والوسائل الأمنية المطبقة من طرف إدارة تكنولوجيا المعلومات بالمؤسسة لتقليل من حدة المخاطر والتهديدات التي يتعرض إليها نظام معلوماتها، حيث توصلت الدراسة إلى أن: مؤسسة "السويدي إلكترونيك الجزائرية" تتعرض للعديد من المخاطر لأسباب متعددة أهمها تلك المتعلقة بقلة الوعي لدى الموظفين، بضعف الرقابة، بالإضافة إلى المخاطر المتعلقة بالبيئة الخارجية وغيرها... كما تم التوصل إلى أن المؤسسة محل الدراسة تولي اهتماما كبيرا بمجال أمن المعلومات، من خلال سعيها الدائم لاقتناء وتطبيق أحدث التكنولوجيات في هذا المجال.

الكلمات المفتاحية: نظام المعلومات، مخاطر، تهديدات، اعتداءات، أمن المعلومات.

تصنيف JEL: D80، D82، D89

Abstract

This study aims to expose the reality of the management of information security within the enterprise "Elsewedy Electric Algeria" to try to highlight the different techniques and security methods applied to reduce the risks and threats to its information system; although; it was concluded that: "Elsewedy Electric Algeria" is exposed to many risks for several reasons, mainly those related to lack of awareness among employees, the weakness of the control measures, the risks related to the external environment. However, we've seen a waning interest in information security, through its ongoing quest for the acquisition and application of the latest technologies in the field.

Key words: Information system, risks, threats, attacks, information security.

Jel Classification Codes : D80 ،D82 ،D89.

المؤلف المرسل: هاجر بوعوة، الإيميل * hadjer.bouaoua@gmail.com

توطئة (مقدمة):

تنشط المؤسسات الجزائرية في بيئة أعمال تمتاز بالديناميكية من حيث سرعة تبادل المعلومات، انفتاح الأسواق، شدة المنافسة والتطور التكنولوجي، إضافة إلى امتيازها بالتعقيد وعدم التأكد الذي جعل المؤسسة الجزائرية تعيش في أوضاع مفاجئة تأتي في شكل أزمات تؤثر سلبا على أدائها، حيث أصبحت أجهزتها وما تحويه من معلومات متاحة لكل من يستطيع الوصول لهذه الأجهزة من خلال الارتباط الحاصل بواسطة الشبكة العنكبوتية، مما يجعل نظام معلوماتها عرضة لمختلف المخاطر المهمة المتعلقة بأمن وتكامل النظم، وأمام هذه الظروف وغيرها، كان ولا بد على هذه المؤسسات التعامل بمجدية مع هذه المخاطر والاعتداءات، من خلال تطبيق تقنيات وأدوات حديثة من شأنها التقليل من أثر هذه الأزمات واسترداد الخسائر، حيث أنه في الواقع لا توجد وسيلة أمنية شاملة على نظام المعلومات ضد كل حادث محتمل. وعلى هذا الأساس جاءت هذه الدراسة التي تسعى بشكل أساسي إلى التطرق لواقع إدارة أمن المعلومات في مؤسسة "السويدي إلكترونيك الجزائر"، والتي جاءت بسبب تزايد الاهتمام الكبير بتوفير الأدوات اللازمة لحماية نظم المعلومات والرقابة على عملياتها وضمان استمرارية عمل تلك النظم بشكل صحيح وبالطريقة المطلوبة التي صممت من أجلها، لكن هذا الاهتمام والتطور في تكنولوجيا المعلومات لم يصاحبه تطور مماثل في الممارسات والضوابط الرقابية، كما لم يواكب ذلك تطورا مماثلا في معرفة وخبرات ووعي موظفي المؤسسة. ومن هنا تظهر مهمة جديدة ومسؤولية كبيرة أمام إدارة تكنولوجيا المعلومات في المؤسسة وهي ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل هذه النظم بشكل صحيح والتخطيط الدقيق لمواجهة جميع الأخطار التي يمكن أن تؤدي إلى تعطيلها أو توقفها عن العمل، وفي حالة حدوث ذلك، التمكن من إعادة تشغيلها بأسرع وقت ممكن، وتسمى هذه الوظيفة المهمة بحماية وأمن نظم المعلومات، والتي تهدف إلى حماية الموارد الحوسبة من المخاطر والتهديدات المقصودة وغير المقصودة التي يمكن أن تؤدي إلى عمليات غير مسموح بها مثل تعديل أو انكشاف أو تخريب البيانات أو البرامج.

● مشكلة الدراسة وأسئلتها:

رغم أن مؤسسة "السويدي إلكترونيك الجزائر"، تعمل على حماية بياناتها ومعلوماتها من السرقة والاختراق وذلك من خلال الإدارة السليمة لأمن معلوماتها وشبكات اتصالاتها، إلا أن المخاطر التي تواجهها كثيرة ومتنوعة، وذلك بسبب التطور التكنولوجي ووسائل تخزين المعلومات وتبادلها بطرق مختلفة. وبهذا سعت مؤسسة "السويدي إلكترونيك الجزائر" إلى مواكبة التطور التكنولوجي ووسائل حماية وأمن المعلومات والبيانات ذات الصلة بعملها وذلك للحد من السرقة والاختراق من خلال الإدارة السليمة لأمن معلوماتها. وعليه، تحدت مشكلة الدراسة في الإجابة على التساؤل الرئيسي التالي: ما هو واقع إدارة أمن المعلومات في مؤسسة "السويدي إلكترونيك الجزائر"؟ ويتفرع هذا التساؤل إلى عدة تساؤلات فرعية تتمثل في ما يلي:

1- هل يتأثر نظام أمن المعلومات بمؤسسة "السويدي إلكترونيك الجزائر" بالمخاطر العملية، المخاطر الإدارية والسياسات والإجراءات؟

2- على ماذا يقوم نظام أمن معلومات مؤسسة "السويدي إلكترونيك الجزائر" حاليا؟

3- هل تسعى مؤسسة "السويدي إلكترونيك الجزائر" لاقتناء وتطبيق أحدث التقنيات في مجال أمن نظم معلوماتها؟

• فرضيات الدراسة:

استنادا إلى مشكلة الدراسة تمت صياغة الفرضيتين التاليتين:

الفرضية الأولى: لا يتأثر نظام أمن المعلومات بمؤسسة "السويدي إلكتروني الجزائر" بالمخاطر العملية، المخاطر الإدارية والسياسات والإجراءات؛

الفرضية الثانية: لا تسعى مؤسسة "السويدي إلكتروني الجزائر" لاقتناء وتطبيق أحدث التقنيات في مجال أمن نظم معلوماتها؛

• أهمية الدراسة:

تستمد هذه الدراسة أهميتها من النقاط الآتية:

1. أن نظم المعلومات قد أصبحت عرضة للعديد من المخاطر التي تهدد صحة وموثوقية ومصداقية وسرية وتكاملية المعلومات إضافة إلى إمكانية إتاحة البيانات التي توفرها تلك النظم، مما يؤدي إلى سهولة حدوث تلك المخاطر؛
2. وجود خلط واضح وعدم التمييز بين مخاطر أمن نظم المعلومات وعدم كفاية الضوابط الرقابية لأمن تلك النظم؛
3. أن معظم الدراسات السابقة أهملت تماما جانب مهم للمخاطر المرتبطة بقلة وعي وتدريب الموظفين وضعف التدابير الرقابية؛
4. حداثة هذه الدراسة وإمكانية إفادة مؤسسة "السويدي إلكتروني الجزائر" لأنها بأمر الحاجة لمثل هذه الدراسة لكونها تتعامل مع العديد من الأنظمة والتطبيقات التي تتركز على أهمية المخاطر التي تواجه أمن نظم المعلومات لديها، وبالتالي تمكن هذا القطاع من الاستفادة من نتائجها؛
5. اعتبار هذه الدراسة نقطة انطلاق لمزيد من الدراسات المستقبلية فيما يتعلق بموضوعها؛

• الدراسات السابقة:

- دراسة (زيدان وحمو، 2010) بعنوان "متطلبات أمن المعلومات المصرفية في بيئة الانترنت"، هدفت إلى إبراز متطلبات تحقيق الأمن المعلومات للبنوك في بيئة الانترنت وسبل مواجهة عمليات الاحتيال المصرفي، مع تسليط الضوء على جهود البنوك في مواجهة القرصنة المعلوماتية، وقد توصلت الدراسة إلى وجود بني تقنية تحتية عالمية تستخدمها المؤسسات المالية والمصارف من شأنها أن تكفل أمن وسلامة عمل هذه المؤسسات، وأن هناك تطورا في مجال تقنية أمن المعلومات للتعامل مع التهديدات الأمنية ذات العلاقة بشبكة الانترنت. كما يوجد نقص في التشريعات والقوانين المنظمة للعمل المصرفي في بيئة الانترنت، وغياب معايير ومبادئ للتجزي والاستعلام، وهو ما يؤدي إلى حدوث حالات احتيال مالي ومصرفي؛

- دراسة (Veiga & Eloff, 2010) بعنوان "A framework and assessment instrument for information security culture"، هدفت إلى وضع إطار لتقييم ثقافة أمن المعلومات وذلك بالاعتماد على الأدبيات السابقة في موضوع أمن المعلومات. وقد توصلت الدراسة إلى وضع إطار لتقييم ثقافة أمن المعلومات في شركات عالية التكنولوجيا في الولايات المتحدة الأمريكية. حيث تضمن هذا الإطار العديد من العوامل ذات الأهمية البالغة ومنها كلمة السر والهوية؛

- دراسة (Huang & al, 2010) بعنوان "Perception of information security"، هدفت إلى فحص إدراك الأفراد لأمن المعلومات وتحديد أهم العوامل التي تؤثر في مستوى إدراكهم للتهديدات المختلفة على أمن المعلومات. تكونت عينة الدراسة من 602 مستجيب لتقييم 21 خطرا في أمن المعلومات. وقد توصلت الدراسة إلى وجود ستة عوامل رئيسية اعتبرها أفراد عينة الدراسة تشكل تهديدا من وجهة نظرهم تتمثل في: قرصنة الكمبيوتر، الديدان، الفيروسات، أحصنة طرواده وبرامج الباب الخلفي؛

- دراسة (بن الطيب، 2018) بعنوان "أهمية أمن نظم المعلومات لدى المؤسسات الاقتصادية الحديثة"، هدفت إلى إبراز مختلف الجوانب المتعلقة بموضوع جرائم الحاسوب، ووصف العديد من أنواعها القادرة على اختراق الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير التطبيقات المخوذة ضمنه، وإبراز مصادر وأنواع المخاطر والتهديدات الأمنية، بالإضافة إلى وصف الأنواع المختلفة من التدابير الأمنية والوقائية المتبعة لحماية البيانات وأنظمة المعلومات. وقد توصلت الدراسة إلى أن تزايد الاعتماد على المعلومات وشبكاتها زاد من تأثير الأخطار التي يمكن أن تواجهها، وأن قضية أمن المعلومات وتبادلها عبر الشبكات ذات أهمية فائقة لتقنيات المعلومات في شتى مجالات الحياة في هذا العصر، يتوجب حمايتها بانتظام، كما توصلت الدراسة إلى أن تحقيق أمن نظم المعلومات بشكل كامل وبنسبة 100% لا يمكن ضمانها، لأن مجال التقنية عبارة عن بيئة متغيرة تجلب كل جديد وفي كل لحظة مخاطر جديدة وغير محدودة لذلك ينبغي أن يكون الهدف هو الحفاظ قدر الإمكان على أمن المعلومات ومتابعة كل ما هو جديد في عالم التكنولوجيا.

● ما يميز الدراسة الحالية عن الدراسات السابقة: إن أهم ما يميز الدراسة الحالية عن الدراسات السابقة يمكن تلخيصه بالاتي:

1. من حيث بيئة الدراسة وقطاع التطبيق: أجريت الدراسات السابقة على المؤسسات الأمريكية بالإضافة لمؤسسة عربية، أما الدراسة الأخيرة أجريت على المؤسسات الجزائرية بشكل عام، في حين تم تطبيق الدراسة الحالية في مؤسسة جزائرية لصناعة الكابلات والمحولات الكهربائية أي في المجال الطاقوي؛

2. من حيث هدف الدراسة: تنوعت الاتجاهات البحثية للدراسات السابقة، والتي هدفت إلى قياس التأثير والعلاقة ووضع مجموعة من المعايير لأمن المعلومات والاتصالات، أما الدراسة الحالية فقد هدفت بشكل أساسي إلى التعرف ودراسة واقع إدارة أمن المعلومات في مؤسسة "السويدي إلكترونيك الجزائر"، إذ ستساعد

هذه الدراسة على تبيان أهم المخاطر التي تهدد أمن المعلومات، بالإضافة إلى تحديد وسائل الحماية الممكنة لذلك؛

3. من حيث المنهجية: يمكن عد الدراسة الحالية دراسة استطلاعية، وصفية واستقرائية لكونها تأخذ وجهة نظر

رئيس إدارة تكنولوجيا المعلومات بالمؤسسة من خلال إجراء مقابلة شخصية معه وتدوين ما تم شرحه كتابيا؛

1. ماهية أمن المعلومات:

يعتبر أمن المعلومات من الركائز الأساسية التي تأخذها المؤسسات بعين الاعتبار وتضخ لها ميزانيات ضخمة، وذلك من أجل التقليل من مختلف المخاطر والاعتداءات التي تواجهها المؤسسات، وبالتالي السماح لها بالتقليل من مختلف الخسائر التي قد تصيبها.

1-1- المخاطر والتهديدات التي تواجه نظم معلومات المؤسسة:

مع تطور التجارة الإلكترونية والاستخدام المتزايد للإنترنت، أصبح هناك تشارك وتبادل أكثر للمعلومات من طرف شركاء الأعمال، على المستويين الوطني والدولي، مما أحدث ثورة في مجال الأعمال، وهنا تكمن المشكلة في ظهور خطر التخريب، التلاعب، المسح أو الاحتيال دون أن تكون المؤسسة على علم بذلك أو ضد إرادتها.

1-1-1- تعريف المخاطر والتهديدات:

من المهم جدا للمؤسسة معرفة وتحديد المتغيرات المختلفة التي قد تضر بها، وتصنيفها في فئتين هي: المخاطر والتهديدات؛

✓ المخاطر: تواجه المنظمة مخاطر عديدة، معقدة ومتنامية، لذا يجب أن تكون على دراية بضرورة أن تكون حذرة، وتعمل في سرية للحماية ضد هذه المخاطر التي يمكن أن تؤثر على أصولها المعلوماتية (Claude & Possin, 2006, p. 85). وعموما يمكن تصنيف المخاطر إلى فئات على أساس موضوعها، بدءاً من المخاطر البيئية، إلى تلك المتعلقة بالسلامة والأمن وهي كالتالي: (Claude & Possin, 2006, p. 14) المخاطر البيئية، المخاطر الأمنية، مخاطر السلامة، المخاطر التنظيمية والإدارية. كما اقترح (Siponen & Baskerville, 2002, pp. 337-346) التصنيف التالي: مخاطر اختراق الأنظمة، الاعتداء على حق التحويل، مخاطر زراعة نقاط الضعف، مراقبة الاتصالات، إنكار/ حجب الخدمة، عدم الإقرار بالقيام بالتصرف.

✓ التهديدات: تعبر التهديدات على وجه الخصوص على النوايا البشرية السيئة. فحسب (Henry Bouchet, 2007, p. 51) أن التهديدات التي تواجه أمن المعلومات تشمل اثني عشرة نقطة وهي: الخطأ أو الفشل البشري، سرقة الحقوق الذهنية والفكرية، أفعال التجسس المتعمدة، أفعال متعمدة لابتزاز المعلومات، أفعال متعمدة للتخريب أو التدمير، أفعال متعمدة للسرقة، هجوم متعمد للبرمجيات، قوى الطبيعة، نوعية انحرافات الخدمة من مجهزي الخدمة، حالات فشل أو أخطاء أجهزة تقنية، حالات فشل أو أخطاء البرامج التقنية، وأخيرا تقادم تكنولوجيا.

1-1-1- أسباب حدوث المخاطر:

تعرض نظم معلومات المؤسسة للعديد من المخاطر التي قد تهدد أمنها وذلك بسبب مجموعة من العوامل والتي يمكن تلخيصها كما يلي (سلطان، 2009، الصفحات 393-394):

1. تتضمن نظم المعلومات كما هائلا من البيانات ولذلك فانه يصعب عمل نسخ ورقية لها؛
2. صعوبة اكتشاف الأخطاء الناتجة عن التغير في نظام المعلومات وذلك لأنه لا يمكن التعامل أو قراءة سجلاتها إلا بواسطة الحاسب الذي لا يكشف أي تغير؛
3. صعوبة مراجعة الإجراءات التي تتم من خلال الحاسب وذلك لأنها غير مرئية وغير ظاهرة؛
4. صعوبة تغيير النظم الآلية مقارنة بالنظم اليدوية؛
5. قد تؤدي المخاطر التي تتعرض لها النظم الآلية إلى تدمير كافة سجلات المنظمة وبذلك فهي أشد خطورة على النظم الآلية من النظم اليدوية؛
6. ضعف الرقابة على النظام الآلي بسبب الاتصال المباشر للمستخدم بنظم المعلومات؛
7. استخدام العديد من التطبيقات في مواقع مختلفة لنفس قاعدة البيانات يؤدي إلى إمكانية اختراقها بفيروسات الحاسب وبالتالي إمكانية تدمير أو تغيير قاعدة البيانات لنظام المعلومات.

1-2- الأشكال المختلفة للاعتداءات التي تواجهها المؤسسة:

من المهم التمييز بين الاعتداءات المادية والاعتداءات الالكترونية:

1-2-1- الاعتداءات المادية:

تتطلب الوصول الفعلي إلى المكان، أو استخدام خصائص ملموسة معينة، وتشمل هذه الاعتداءات: الاعتراض، التشويش، التجسس، التزوير المادي، الولوج غير شرعي (Henry Bouchet, 2007, pp. 56-57)؛

1-2-2- الاعتداءات الالكترونية:

يعتبر اختراق الحواسيب ونظم المعلومات أو الاعتداء عليها عبر الانترنت من أكبر سلبات الشبكة والتي تعوق الحركة فيها وتتطلب الحذر، والمشكلة تكمن في وجود الكثير من البرامج التي تقوم بعمليات الاختراق والتي لا تتطلب من المستخدم خبرة كبيرة في مجال الشبكات. وهذه النوعية من البرامج موجودة بكثرة ومجانا في الانترنت؛ ويمكن تلخيص مختلف أشكال الاعتداءات الالكترونية حسب (Jakobiak, 2004, p. 32) كما يلي:

- القرصنة: ونجد في هذا النوع الأول:
 - المتسللون: وهم عادة يقومون بالاختراق بغرض اللعب أو التحدي، ولا يعتمدون الإيذاء وإلحاق الضرر، ومع ذلك قد يكونوا خطرين؛
 - المخترقون: وهم المحترفون في القرصنة، الذين يسعون لإلحاق الأذى، وهم يعرفون كيفية الاعتداء ومهاجمة مفتاح الدخول؛

- المدمرون: وهم المخربون الحقيقيون، يتحركون بشكل دائم مع نية إلحاق الأذى والتدمير، وهم يعتبرون خطيرون بشكل خاص؛
- المتطفلون: وهم المتخصصون في الدخول إلى الشبكات الهاتفية من أجل أن يتمكنوا من التواصل مجانا عبر جميع أنحاء العالم، علاوة على ذلك، الوصول إلى الرسائل الموجودة في صناديق البريد الصوتي لموظفي المؤسسة؛
- الاعتداءات المنطقية: نجد في هذا النوع جميع البرامج والبرمجيات التي يتم تداولها على الشبكة والتي تتمثل في:
 - البرامج الخبيثة: تستخدم لتعطيل عمل الشبكات والحاسبات بالإضافة إلى تدمير المواقع الالكترونية المختلفة وسرقة المعلومات السرية وغيرها من الأعمال غير المشروعة كإنجاز احتيال أو غش في نظام المعلومات، وتشمل أنواعا عديدة يمكن تلخيصها فيما يلي: (مسوس و حديد، 2016، صفحة 33) الفيروسات، حصان طروادة، الدودة، الهوكس Houks، القنبلة المنطقية، هجمات حجب الخدمة.
 - برامج الجوسوسة (spyware): وهي عبارة عن برامج تستغل في الاستخدام غير المشروع للمعلومات من خلال تثبيتها بداخل النظام، حيث تتواصل مع وكيل خارجي عن طريق ما يعرف بالباب الخلفي (Laurent & Wolfhugel, 2011, p. 37)
 - برمجية الرصد (المراقبة): عملها مثل عمل الشيطان، حيث تم تطويرها من قبل متخصصين في أمن المعلومات، للكشف عن الثغرات الموجودة ضمن شبكة المنظمات بغرض الاستفادة منها بطريقة غير شرعية، حيث يعتمد هذا الأسلوب على برامج خاصة تدعى برمجيات sniffers: التي تقوم باعتراض وتحليل البيانات المتنقلة داخل الشبكة (بعد إرسالها من قبل المرسل وقبل استقبالها من طرف المستقبل) (Laurent & Wolfhugel, 2011, p. 38)
 - كوكيز cookie: وهو عبارة عن تسجيل للمعلومات من قبل الخادم في ملف خطي موجود في جهاز كمبيوتر العميل، فمعلومة نفس الخادم يمكن أن يقوم بإعادة قراءتها وتعديلها فيما بعد؛
 - سبام (Spam) (Spiced Pork And Meat): ويشير إلى صعوبة هضم البرنامج للكميات الضخمة من البيانات التي تقوم هذه البرامج بإرسالها وإغراق خوادم الويب بها دفعة واحدة لتعطيلها؛
 - الصيد الاحتيالي phishing: وهو عبارة عن إرسال مئات الآلاف من الرسائل الالكترونية غير مرغوب فيها الخوادم البريد الالكتروني دفعة واحدة لأجل إيقافها عن العمل وذلك انطلاقا من حاسب واحد فقط، وإنشاء مواقع مزيفة للحصول على بيانات شخصية ومالية، ويمكن القيام بهذا الاعتداء بالاستعانة بالعديد من حاسبات مستخدمي الانترنت، وبدون إرادتهم؛

1-2-3- أشكال أخرى للاعتداءات:

بالإضافة إلى ما سبق، هناك مجموعة أخرى من الاعتداءات حسب (Claude & Possin, 2006, p. 36) تتمثل في: التجسس، الاضطراب، التخريب، سرقة البيانات، سرقة الموارد، التزامن، تحليل التشفير.

1-3- تعريف أمن المعلومات:

يعرف أمن المعلومات بأنه "السياسات والإجراءات والمقاييس الفنية التي تستخدم لتحويل دون الوصول غير المعتمد أو السرقة أو التدمير للسجلات" (سلطان، 2009، صفحة 396)؛ كما تم تعريفه أيضا بأنه عبارة عن "السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة لتداول حركات الأعمال الكترونيا عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الالكتروني وعلى شركات الأعمال والزبائن والمنظمين والمستفيدين وأي شخص آخر ممكن أن يكون معرضا لمخاطر الاختراق" (صادق و الفتال، 2008، صفحة 11).

1-4- أهداف أمن المعلومات:

إن الهدف من أمن المعلومات لا بد أن يتفق مع أهداف المؤسسة، ولكي يتم ذلك لا بد من تحقق مجموعة من المتطلبات، وهي: (مسوس و حديد، 2016، صفحة 35)

- **سرية المعلومات:** من خلال العمل على أن لا يطلع عليها من قبل المستخدمين غير المخولين بذلك، بمعنى آخر حمايتها من الاعتراض والنشر غير المرخصين؛
 - **سلامة المعلومات:** من خلال العمل على أن يبقى المحتوى على حاله بدون أي تعديل أو حذف غير مشروعين، أو بمعنى آخر ضمان صحتها وكمالها؛
 - **توافر البيانات أو الخدمة:** من خلال العمل على إتاحة كل منهما للمستخدمين المرخصين عند الطلب، وذلك بعد تطبيق العمليات الخاصة بأمن المعلومات؛
- ولتحقيق المتطلبات الثلاثة سابقة الذكر، أكد (الجنهبي و الجنهبي، 2006، صفحة 13) أن المنظمات تحتاج إلى استخدام مجموعة من المقاييس، وتندرج هذه المقاييس تحت ثلاثة أمور رئيسية هي:

1. **التحكم بالوصول:** التي تمكن من التحكم بمكونات البرامج أو مكونات الأجهزة من حيث المنع أو السماح للوصول إلى مصادر الشبكة ويمكن تمثيلها بالبطاقات الذكية أو أجهزة البصمة أو تكون أجهزة الاتصال الشبكي مثل نقاط الوصول للأجهزة اللاسلكية بتخصيص صلاحيات على ملفات شخصية لمستخدمي الكمبيوتر؛

2. **إثبات الصلاحيات:** وهي عملية التحقق من صلاحيات المستخدمين على مصادر الشبكة ويتم تحديد المستخدم من خلال استخدام اسمه وكلمة السر أو البطاقات الذكية ويتم بعد ذلك إعطاؤه الصلاحيات يتم تحديدها من قبل مدير الشبكة بناء على هويته؛

3. **التدقيق:** وهي عبارة عن عمليات التأكد وتتبع الصلاحيات عن طريق مراقبة الموارد والشبكة وتعتبر من أهم الأمور في مجال أمن الشبكة حيث يتم التعرف على المخترقين ومعرفة الطرق والأدوات التي تم استخدامها للوصول إلى الشبكة؛

1.1. متطلبات إدارة أمن المعلومات:

إن مسألة أمن نظم المعلومات من المسائل المهمة والضرورية التي ينبغي على المؤسسة أخذها بعين الاعتبار، لذلك توجد عدة متطلبات لإدارة أمن نظم المعلومات تتمثل في:

1-1- وضع سياسة أمن معلومات خاصة بالمؤسسة:

في الواقع، يعد تأمين وتوثيق المعلومات جزءا من الرغبة في التقليل من المخاطر وحالات عدم التأكد. فمن الضروري إشراك اللجان والجهات الفاعلة من خلال إنشاء سيورة تجمع عدة مراحل (Claude & Possin, 2006, p. 157)، ولا بد من الاعتماد على مجموعة من المعايير الدولية الخاصة بأمن المعلومات والمتمثلة في معايير ISO 27000، وهي مجموعة من المعايير الموضوعة تحت تصرف المنظمات التي ترغب في تحديد المقاييس اللازمة في إطار سيورات تنفيذ نظام إدارة أمن المعلومات (ISMS)، الذي يتضمن على وجه الخصوص (Benjamin, 2009, p. 9) :

1-1-1- ISO/IEC 27001:

وهو يحدد المتطلبات المتعلقة بنظام إدارة أمن المعلومات الخاصة بالمؤسسة (ISMS)، لتنفيذ تدابير أمن المعلومات المعترف بها عالميا ووضع التعليمات الخاصة بإدارة أمن المعلومات. ويمكن تلخيص فوائد تطبيق معيار ISO 27001 في النقاط التالية (Benjamin, 2009, p. 11) :

- ✓ المحافظة على ممتلكات المؤسسة سواء كانت معنوية مثل المعلومات والبرامج أو مادية كالأجهزة والمباني؛
- ✓ زيادة الوعي لجميع موظفي المؤسسة بأهمية أمن المعلومات والنتائج السلبية المترتبة بعدم الالتزام بذلك؛
- ✓ الالتزام بمعيار ISO 27001 وبالمواصفات عموما دليل على اهتمام المؤسسة بتطوير أدائها وحرصها على الالتزام بأعلى المعايير لتقديم أفضل السلع والخدمات؛
- ✓ زيادة التنافسية للمؤسسة مقارنة بالمؤسسات الأخرى العاملة في نفس المجال؛
- ✓ جاهزية المؤسسة على مواصلة أدائها في حالة حصول الحوادث الطارئة الطبيعية.

1-1-2- ISO/IEC 27002:

استبدال المعيار 17799 في 1 جويلية 2007، وهو يخص الممارسات الجيدة التي تقدم إرشادات حول المعايير التنظيمية المتعلقة بأمن المعلومات والممارسات الجيدة لإدارة أمن المعلومات، بما في ذلك اختيار وتنفيذ وتسيير التدابير الأمنية التي تأخذ بعين الاعتبار بيئة مخاطر أمن معلومات المنظمة؛

ومنه فان مجموعة معايير ISO 27000 ضمن المنظمة العالمية للتقييس تهدف لتلائم استخدامات متنوعة وهي كالتالي (Jacobs, 2011, p. 170) :

- ✓ يستخدم داخل المؤسسات لتشكيل الأهداف والمطالب الأمنية؛
- ✓ التوافق مع التشريعات والقوانين؛
- ✓ التعرف على إجراءات جديدة لإدارة أمن المعلومات؛

- ✓ يستخدم من قبل الإدارة لتحديد وضعية النشاطات الأمنية؛
- ✓ يحدد المدققين الداخليين والخارجيين من خلاله مستوى التوافق مع السياسات والإجراءات المقررة.

II-2- وسائل أمن المعلومات:

تتمثل أهم وسائل أمن المعلومات في (الشاعر، 2004، صفحة 435):

- ✓ **الاكتشاف المبكر للاختراقات:** ويتم ذلك عن طريق ملف تسجيل النظام، الأوامر، نظام التشغيل، ومدير المهمات الذي يعرض جميع البرامج ويتم التعرف على البرامج الدخيل من بينها؛
- ✓ **حماية الشبكة:** يتم حماية الشبكة داخليا باتخاذ مجموعة من الإجراءات منها تدريب العاملين في الشبكة على التعامل مع الإجراءات الأمنية المتبعة في المنظمة التي تحوي الشبكة؛
- ✓ **التشفير المحكم:** يمثل التشفير الوسيلة الأكثر أهمية لضمان سرية وموثوقية وسلامة البيانات المتبادلة. فالتشفير يدخل في مختلف الوسائل التقنية التي تعمل على تحقيق حماية هذه العناصر، ويعد التشفير بوجه عام وتطبيقاته العديدة وفي مقدمتها التواقيع الالكترونية، الوسيلة الوحيدة تقريبا لضمان عدم إنكار التصرفات عبر شبكات الحاسبات. ويعتمد التشفير على تغيير محتوى الرسالة باستخدام ما يسمى بمفتاح التشفير وذلك قبل إرسال الرسالة على أن تكون لدى المستقبل القدرة على استعادة محتوى الرسالة في صورتها الأصلية باستخدام مفتاح فك الشفرة. ولضمان كل من سرية وموثوقية وسلامة البيانات والرسائل المتبادلة يستعمل عادة أسلوبين وهما: أسلوب الشبكة الخاصة الافتراضية و أسلوب الأمن من خلال نظام SSL (مسوس و حديد، 2016، صفحة 37)؛

- ✓ **الجدار المقاوم للنار:** يقوم جدار النار بترشيح البيانات المدخلة والمخرجة، بحيث يعوق تدفق البيانات بين شبكات المنظمة والانترنت. والفكرة من وراء هذا النوع من الجدران هي أنها تحقق أمنا واحدا لكل الحاسبات المرتبطة بالشبكة بدلا من أمن مستقل لكل حاسب؛ كما يمكن تقسيم الجدران المقاومة للنار إلى نوعين أساسيين هما: (مسوس و حديد، 2016، صفحة 37)

- **الجدران البرمجية المقاومة للنار:** يمكن استعمال هذا النوع من الجدران على الحاسبات المستقلة أو الحاسبات المرتبطة بالشبكة أو على الخوادم؛
- **الجدران المادية المقاومة للنار:** تسمى كذلك بالعلب السوداء، وهي تستعمل عادة على الخوادم، وهي أكثر أمنا من الجدران البرمجية، لكونها غير معنية بنقاط ضعف نظام تشغيل الحاسب أو بمختلف ثغراته؛
- ✓ **مضادات الفيروسات:** وهي مجموعة البرامج التي تتصدى للفيروسات الداخلة إلى الجهاز، وتتفاوت مضادات الفيروسات من حيث القوة والفاعلية إلا أنه يمكن لصناع الفيروسات ونشرها تجاوز مفعولها في كثير من الأحيان؛

- ✓ **تعدد الخوادم:** ويقصد بتعدد الخوادم استخدام خادم لكل نظام أو لكل مجموعة أنظمة تربطها علاقة وظيفية مثل التعاميم، المعاملات السرية، اللوائح والقوانين، التحقيقات، المطلوبين، الشؤون الإدارية، شؤون الضباط

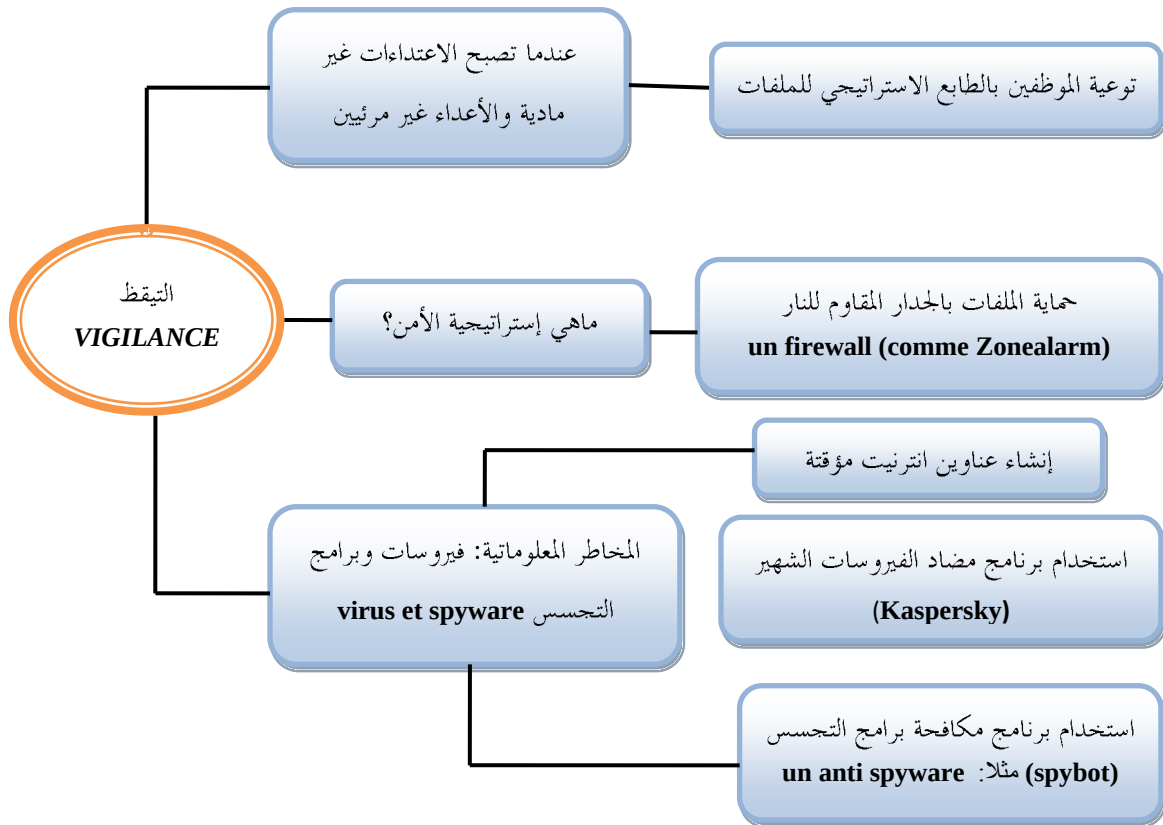
والأفراد، حيث أن تواجد جميع هذه الأنظمة في خادم واحد يزيد من احتمال اختراقها وتوزيع جميع الأنظمة وتعددتها يؤدي إلى انحصار المشكلة في خادم واحد ونظام واحد.

11-3- خطة حماية أمن المعلومات:

من الضروري وضع خطة حماية شاملة في حدود إمكانيات المؤسسة التنظيمية والمادية، ويجب أن تكون تلك الحماية قوية وليست ضعيفة، والتي تتمثل في:

- ✓ وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمل وتطبيقات المؤسسة؛
 - ✓ يجب على الإدارة العليا في المؤسسة دعم أمن نظم المعلومات لديها؛
 - ✓ يجب أن توكل مسؤولية أمن نظم المعلومات في المؤسسة لأشخاص محددين؛
 - ✓ تحديد الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة؛
 - ✓ تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية؛
 - ✓ الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل آمن؛
 - ✓ تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط؛
 - ✓ تأمين استمرارية عمل وجاهزية نظم المعلومات خاصة في حالة الأزمات ومواجهة المخاطر المتعلقة بنظم المعلومات؛
- والشكل رقم 1 الموالي يوضح تركيبة السياسة الأمنية لضمان أمن معلومات المؤسسة:

شكل رقم (1): يوضح تركيبة السياسة الأمنية لضمان أمن معلومات المؤسسة



المصدر: من إعداد الباحثين.

111. الطريقة والأدوات:

للإجابة على إشكالية الدراسة، واثبات صحة الفرضيتين المتبنتين من عدمها، ولطبيعة موضوع الدراسة الذي يرمي إلى دراسة واقع إدارة أمن المعلومات في المؤسسة الجزائرية، اخترنا أسلوب المقابلة مع رئيس مصلحة إدارة IT، حيث كان موضوع المقابلة متعلق فقط بنشاطات أمن المعلومات بالمؤسسة، بغية الوقوف على معرفة مختلف المخاطر التي تؤثر على نظام معلومات المؤسسة، بالإضافة إلى إبراز السياسات والإجراءات المطبقة من قبل إدارة أمن المعلومات؛

• حدود الدراسة:

تمثلت حدود الدراسة بما يلي:

الحدود المكانية والزمانية: لقد تمت الدراسة التطبيقية على مستوى إدارة تكنولوجيا المعلومات IT في مؤسسة "السويدي إلكترونيك الجزائر" الكائن مقرها في المنطقة الصناعية بعين الدفلى، أما فيما يخص الإطار الزمني فتتمت في مدة يوم واحد 2019/03/14، حيث استخدم الباحثين أسلوب المقابلة بهدف جمع المعلومات واختبار الفرضيتان السابقتان، في حين استغرقت المقابلة مدة ساعتين؛

الحدود البشرية: تم نقل المقابلة بالكامل على أساس تدوين كتابيا ملاحظات المستجوب السيد "عيادي سيد علي"، وهو يشغل منصب رئيس مصلحة إدارة تكنولوجيا المعلومات IT (ذي 12 سنة خبرة).

الحدود العلمية: اعتمد الباحثين على متغيرات أمن المعلومات المتضمنة: إدخال البيانات، التشغيل، المخرجات والبيئة المحيطة، قلة الخبرة والتدريب والوعي للموظفين عدم وجود سياسات واضحة وضعف الإجراءات الرقابية المطبقة؛

111-1- عرض عام لمؤسسة "السويدي إلكترونيك الجزائر"

قامت مؤسسة السويدي إلكترونيك الأم بمصر ببناء أول مصنع لها في الجزائر بالضبط في ولاية عين الدفلى عام 2006، باستثمارات كبيرة قدرها 100 مليون دولار تغطي مساحة 5 هكتارات. وتم تشغيل المصنع ومزاولة المؤسسة نشاطها الفعلي في أكتوبر من عام 2008، ويحتل مصنع عين الدفلى موقعا استراتيجيا في النمو الديناميكي حيث استطاع هذا الفرع أن يبنى لنفسه موقعا هاما في عالم الصناعة وتخصص في مجال الكهرباء، ويعتبر من أفضل فروع السويدي إلكترونيك، حيث يتربع على مساحة قدرها خمسة هكتارات بطاقة إنتاجية تقدر بـ 30.000 طن من الكابلات النحاسية والألمنيوم بما في ذلك كابلات ذات جهد منخفض وكابلات أجهزة الناقل مصنع المحولات و آخر مشروع مصنع اللواحق (الاكسسوارات)، وتقسم إنتاجها بـ 50% من الإنتاج المحلي، و 50% للتصدير، وقد استطاع هذا الفرع أن يبنى لنفسه موقعا استراتيجيا هاما في عالم الصناعة والتخصص في مجال الكهرباء. ويوفر الفرع قوة بشرية تقدر بـ 700 عامل منهم أعوان التنفيذ، أعوان التحكم، وإطارات سامية و مدراء من أجل توفير حل كامل للطاقة؛ ويتمثل نشاط المؤسسة بإنتاج الكابلات الكهربائية ونشر الألياف البصرية، كابل الألياف البصرية تحت الجهد، ومن أهم ما تنتجه المؤسسة:

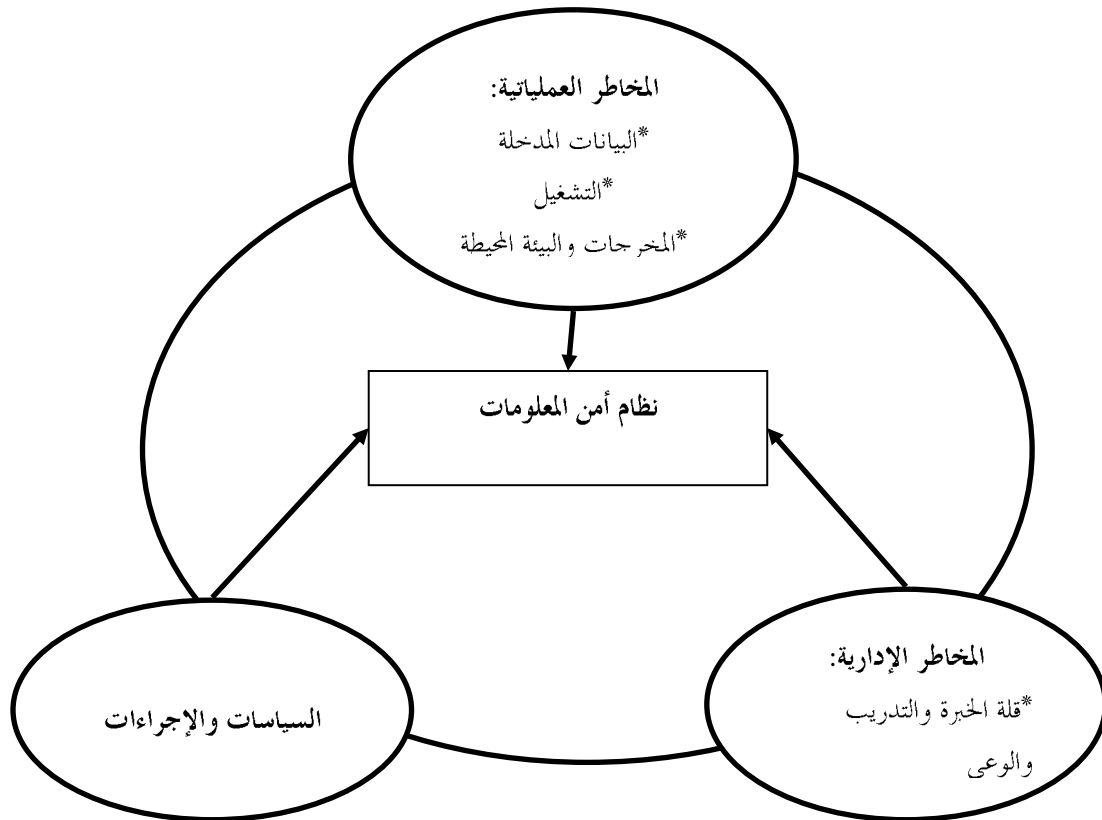
- كابلات الضغط المنخفض: هي الكابلات التي يستعملها المستهلك النهائي لإنارة المساكن والماكينات... وتقدر طاقتها الإنتاجية بـ 20 ألف طن سنويا.
- كابلات الضغط المتوسط: تقدر طاقتها الإنتاجية بـ 3000 كلم سنويا.
- كابلات الضغط العالي: وتقدر طاقتها الإنتاجية 15000 كلم سنويا.
- المحولات الكهربائية: طاقتها الإنتاجية تقدر بـ 3000 محول سنويا.
- كابلات OPGW: تقدر طاقتها الإنتاجية بـ 3000 كلم سنويا.

كما تسعى المؤسسة دائما لاقتناء أحدث التقنيات في مجال أنظمة المعلومات وأمنها، مما يعتبر عاملا أساسيا للحفاظ على درجة وجودة عالية لأداء أنظمة المعلومات وأمنها؛ حيث صممت شبكات مؤسسة "السويدي إلكترونيك الجزائر" أساسا باستخدام شبكات ومعدات الحماية من قبل شركة CISCO.

III-2- نموذج الدراسة:

سيكون نموذج الدراسة مرتكز على المتغيرات المبينة في الشكل رقم (02) الموالي:

شكل رقم (02): نموذج الدراسة



المصدر: من إعداد الباحثين

يمثل نموذج الدراسة العناصر الأساسية التي تؤثر على أمن المعلومات، وهي المخاطر التشغيلية التي تتضمن (البيانات المدخلة، التشغيل، المخرجات والبيئة المحيطة)، والمخاطر الإدارية والمتضمنة (قلة الخبرة والتدريب والوعي،

ضعف الإجراءات الرقابية، بالإضافة إلى المخاطر المتعلقة بالسياسات والإجراءات. إذ إن تكامل هذه المخاطر يهدد أمن المعلومات في المؤسسات كافة كما هو الحال في مؤسسة "السويدي إلكترونيك الجزائر".

1V. النتائج ومناقشتها

يهدف هذا المحور إلى عرض النتائج التي تم التوصل إليها من خلال المقابلة التي أجريت مع رئيس إدارة تكنولوجيا المعلومات حول العناصر الأساسية التي تؤثر على أمن المعلومات التي تظهر في نموذج الدراسة وفقا للتالي:

1V-1- المخاطر التي تؤثر على نظام أمن المعلومات بمؤسسة "السويدي إلكترونيك الجزائر":

يمكن تلخيص أهم المخاطر التي تؤثر على نظام أمن المعلومات بمؤسسة "السويدي إلكترونيك الجزائر" في النقاط التالية (عيادي، 2019):

1V-1-1- المخاطر المتعلقة بالبيانات الداخلة:

ترتبط إما بالإدخال أو بالتدمير غير المتعمد للإجراءات المتعلقة بالبيانات. وهو ما يبين الحاجة الماسة إلى تدريب كافة العاملين ذي العلاقة بحجم الأهمية للبيانات المتعلقة بالعمل وبالتالي العمل على توضيح آليات المحافظة على البيانات؛

1V-1-2- المخاطر المتعلقة بالتشغيل:

ترتبط إما بكلمة السر أو بالإدخال أو اعتراض وصول البيانات إلى أجهزة المستخدمين، وهو ما يتطلب من المؤسسة تزويد العاملين ذي العلاقة فقط ومن توليهم المؤسسة ثقة عالية بكلمة السر وذلك للوصول إلى البيانات المهمة والتمكن من وصول كافة البيانات إلى أجهزة المستخدمين؛

1V-1-3- المخاطر المتعلقة بالمخرجات والبيئة المحيطة :

ترتبط بالمخرجات غير الصحيحة والكوارث الطبيعية كالحرائق وغيرها؛

1V-1-4- المخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين:

ترتبط بالمطبوعات والمعلومات والوثائق غير المخولين بالوصول إليها. وهذا يتطلب عدم السماح باستخدام أقراص ممغنطة بأنواعها وذلك للحد من دخول الفيروسات إلى أنظمتها بالإضافة إلى القيام بالتحديث المستمر لبرمجيات الفيروسات المستخدمة من قبل المؤسسة ووضع ضوابط على الموقع الإلكتروني للحد من الاختراقات التي من الممكن أن تحدث؛

1V-1-5- المخاطر المتعلقة بضعف الإجراءات الرقابية :

ترتبط بثلاثة عناصر رئيسية هي: الفيروسات المدخلة للأنظمة، عمل نسخ غير مصرح بها من المخرجات والكشف غير المرخص به للبيانات.

1V-2- نظام أمن المعلومات في مؤسسة "السويدي إلكترونيك الجزائر":

يقوم نظام أمن المعلومات حاليا في "مؤسسة السويدي إلكترونيك الجزائر" على الآتي (عيادي، 2019):

1-2-1V- إستراتيجية وسياسات أمن المعلومات بمؤسسة "السويدي إلكترونيك الجزائر":

وهي عبارة عن الأنظمة والقوانين التي تحكم أمن معلوماتها، والتي يتم دعمها من قبل المديرية العامة؛

1V-2-2- شبكة المنطقة المحلية LAN:

وهي شبكة نطاق محلية، تكون محتواة داخل مكتب، أو مجموعة من المكاتب داخل بناية واحدة، وتقدم هذه الشبكات سرعة كبيرة لتبادل البيانات والموارد مما يشعر المستخدم أن هذه الموارد موجودة على جهازه الشخصي. ومن سلبيات هذه الشبكة أنه في حالة انقطاع خط الفايبر الرئيسي المغذي للأقسام فسوف تنقطع الخدمة ولا يوجد خط احتياطي لتغذية الأقسام مما يؤدي إلى توقف العمل. وفي حالة انقطاع خط الفايبر المتصل بين المكاتب الرئيسي وباقي المكاتب سوف يتوقف العمل لفترة وجيزة لحين تشغيل المكروريف. وفي العموم عند أي خلل للفايبر سوف يؤثر ذلك على العمل من ضياع للوقت وخسائر للأموال؛

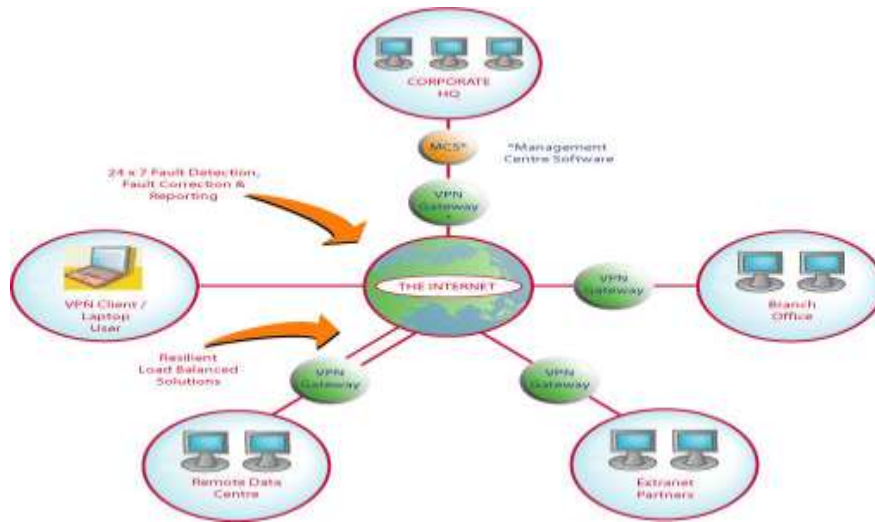
1V-2-3- الشبكات اللاسلكية Wi-Fi :

وهي شبكة تعتمد على موجات الراديو لتبادل المعلومات بدلا من الكابلات التقليدية. حيث يمكن استخدام جهاز الكمبيوتر بدون أن يتصل بكابل الشبكة؛

1V-2-4- الشبكة الخاصة الافتراضية VPN:

وهي عبارة عن قناة اتصال موثقة ومشفرة تمتد عبر شبكة عامة، كشبكة الانترنت، حيث يتم حماية البيانات أثناء النقل بتشفيرها، وتعتمد هذه الشبكة على بروتوكول خاص يعرف باسم **Point-to Point Tunneling Protocol**.

شكل رقم (03): مكونات الشبكة الخاصة الافتراضية في مؤسسة "السويدي إلكترونيك الجزائر"



المصدر: اعتمادا على وثائق المؤسسة

ومن خصائصها أنها تعمل بصورة مستقلة عن خدمة الاتصال المعتادة، حيث أن جميع المعلومات المتبادلة بين الجهازين المضافين يتم نقلها عبر هذه القناة المشفرة، وبالتالي يتحقق الأمان لعدم اختراق المعلومات أو تخريبها. كما

تمكن المستخدمين البعيدين بغض النظر عن مكان تواجدهم من الاتصال والتعامل مع شبكة المؤسسة الخاصة كما لو كانوا في مقر المؤسسة، وتعمل على تأمين الشبكة من خلال إضافة خدمات التشفير. بالإضافة إلى زيادة الإنتاجية من خلال السماح للمستخدمين بالوصول إلى مصادر الشبكة مباشرة مما يسمح لهم بالعمل بفاعلية أكبر عما كان سيحدث إذا كان العمل سيتم عبر البريد الإلكتروني أو التليفون أو بالانتقال إلى مكاتب المؤسسة، الأمر الذي يوفر أموالاً كثيرة. ويوضح الشكل رقم (3) مكونات الشبكة الخاصة الافتراضية في مؤسسة "السويدي إلكتروني الجزائر" (عيادي، 2019)؛

IV-2-5- الجدار المقاوم للنار Pare-feu: فيما يتعلق بمؤسسة "السويدي إلكتروني الجزائر" هناك طبقتان من جدار النار تؤمنان الشبكة المحلية من الاختراق، وهي:

- **جدار النار سمانتك Symantec:** وهو عبارة عن بوابة أمنية تحمي شبكة المؤسسة من الاختراق غير القانوني عبر قوانين مبرمجة ومن الهجمات مثل الفيروسات، ومن فوائد ومميزات هذا الجدار أنه مناسب لاحتياجات المؤسسة بغض النظر عن حجم العمليات، والذي يزيد من فاعلية حماية الشبكة ؛
- **جدار النار سيسكو Cisco:** ومن مميزاته استخدام الشبكة الخاصة الافتراضية، والحماية من الاختراقات بأنواعها المختلفة، وتصفية ومراقبة التصفح عبر الانترنيت؛

IV-2-6- البريد المتطفل Spams:

إذ تعتمد المؤسسة على برنامج Symantec في الحد من البريد المتطفل على خادم البريد الإلكتروني ولكن مازال برنامج Symantec بدائياً جداً في صد البريد المتطفل، ومازالت المؤسسة في طور تقييم بعض المنتجات، وقد تم تجربة بعض المنتجات مثل Xtream.

IV-2-6- الموجهات: وهو عبارة عن جهاز متعدد المنافذ يحدد كيفية معالجة محتويات مجموعة البيانات بناء على البروتوكول وبيانات المؤسسة، إذ تتعدد أنواع الموجهات في المؤسسة، ويقدم الموجه الخدمات التالية لشبكة الـ LAN، وهي إمكانية الإرسال والاستقبال عبر الشبكة في نفس الوقت، وإمكانية وجود العديد من الاتصالات المتزامنة، ودعم للشبكات ذات السرعة العالية، تتميز بوجود مقدار تأخير منخفض ومعدلات عالية من البيانات، وتخصيص سرعة تدفق البيانات تبعاً للمنفذ.

V. الخلاصة:

يمكن القول أن الحاجة المتزايدة للاتصال في مؤسسة "السويدي إلكتروني الجزائر" أدت إلى خلق عصر المعلوماتية الموزعة والمتراصة عبر شبكة الانترنيت، حيث ليس فقط لا تستطيع المؤسسة الاستغناء عن المعلوماتية لعملها الداخلي، ولكن لعملها الخارجي أيضاً، من خلال نظام معلوماتها الذي يسمح لها بالعمل في شبكة مع مورديها، مقاوليها وشركائها والإدارة. وبالتالي تؤدي هذه الحاجة للاتصال الداخلي والخارجي إلى تعرض أنظمة المؤسسة الداخلية لاعتداءات متعددة. كما أن تعميم الأدوات النقلة في مؤسسة "السويدي إلكتروني الجزائر" مثل: (الهواتف المحمولة، آي باد، آي فون، الأندر ويد، الحواسيب المحمولة)، يزيد من حدة تعرضها أكثر لهذه المخاطر، كما لا ننسى

ضعف نظم الرقابة لديها، وقلة تحسيس وتدريب الموظفين بخطورة هذه المخاطر الذي أدى لقلّة وعيهم وتعرضهم لمختلف الاعتداءات. مما أدى بها لتبني تدابير الحماية المتجانسة؛ حيث تقوم بتنفيذ خطة لأمن نظم وتبادل معلوماتها باستعمال مختلف التقنيات والوسائل الحديثة، فالاستثمارات التي قامت بها للتخفيف من هذه المخاطر أقل بكثير من العواقب المالية الناتجة من هذه الاعتداءات، حيث أن مؤسسة "السويدي إلكترونيك الجزائر" تولي اهتماما كبيرا بمجال أمن نظم معلوماتها.

ومن أبرز النتائج المتوصل إليها من خلال هذه الدراسة الميدانية، تتمثل فيما يلي:

■ أن نظام أمن المعلومات بمؤسسة "السويدي إلكترونيك الجزائر" يتأثر بالمخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين؛

■ هناك ضعف في نظم الرقابة في المؤسسة وعدم فعاليتها؛

■ المخاطر المتعلقة بالبيانات المدخلة، والمتعلقة بالتشغيل من شأنها أيضا أن تهدد أمن نظم المعلومات في مؤسسة "السويدي إلكترونيك الجزائر"،

■ للمخاطر المتعلقة بالبيئة المحيطة أهمية كبيرة في إحداث تهديدات على أمن نظم معلومات مؤسسة "السويدي إلكترونيك الجزائر"؛

■ بالرغم من سعي مؤسسة "السويدي إلكترونيك الجزائر" لتطبيق أحدث التكنولوجيات في مجال أمن المعلومات، إلا أن نظام معلوماتها معرض لمختلف المخاطر والتهديدات المحتملة بسبب المخاطر المتعلقة بالسياسات والإجراءات المتخذة؛

■ تولي مؤسسة "السويدي إلكترونيك الجزائر" اهتماما كبيرا بإجراءات الحماية والأمن المعلوماتي، كما تخصص ميزانية معتبرة في هذا المجال؛

■ تستفيد مؤسسة "السويدي إلكترونيك الجزائر" من خبرة المؤسسات العالمية في مجال أمن المعلومات.

ومن خلال النتائج المتوصل إليها في ضوء الدراسة الميدانية، يمكن تقديم مجموعة من الاقتراحات المتمثلة في ما يلي:

■ ضرورة قيام الإدارة بالعمل على خفض حدوث المخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين، وذلك من خلال تدريبهم وتأهيلهم وتوعيتهم بشكل مستمر في مجال أمن المعلومات؛

■ ضرورة قيام الإدارة بشكل دوري بتقييم المخاطر المحتملة للدراية بما يجب عمله عند حدوث مشكل لأمن نظم المعلومات؛

■ يجب تخصيص إدارة لأمن نظم المعلومات، وهذا لتطبيق الأمن المعلوماتي في المؤسسات؛

■ السعي للحصول على معيار Iso27001 فهو التطبيق الأمثل لأمن نظم المعلومات بالمؤسسات؛

■ تحسين مستويات الإجراءات الرقابية؛

■ ضرورة وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمل وتطبيقات مؤسسة "السويدي إلكترونيك الجزائر"؛

■ العمل على توكيل مسؤولية أمن نظم المعلومات في مؤسسة "السويدي إلكترونيك الجزائر" لأشخاص مؤهلين ذوي خبرة في مجال أمن نظم المعلومات؛

VI. قائمة المراجع:

● قائمة المراجع باللغة العربية:

- ابراهيم بن الطيب. (مارس، 2018). أهمية أمن نظم المعلومات لدى المؤسسات الاقتصادية الحديثة. مجلة التنمية والاقتصاد التطبيقي (03)، الصفحات 34-48.
- ابراهيم سلطان. (2009). نظم المعلومات الإدارية: مدخل النظم. الاسكندرية: القاهرة: الدار الجامعية للطبع والنشر والتوزيع.
- دلال صادق، و حميد ناصر الفتال. (2008). أمن المعلومات. الأردن: دار اليازوري.
- زيدان، و حمو. (2010). متطلبات أمن المعلومات المصرفية في بيئة الأنترنت. الرياض.
- سيد علي عيادي. (14 مارس، 2019). المخاطر التي تتعرض لها المؤسسة والسياسة الأمنية المتبعة (مقابلة شخصية). (هاجر بوعودة، المحاور) الجزائر : جامعة الجزائر 3.
- عبد الرحمن بن ابراهيم الشاعر. (2004). تقنية المعلومات والاتصالات. الرياض: المملكة العربية السعودية: دار ثقيف للنشر والتأليف.
- كمال مسوس، و نوفيل حديد. (2016). مقاربات حماية أنظمة معلومات المؤسسة من الاعتداءات الالكترونية. المؤسسة ، الصفحات 26-43.
- منير محمد الجنهبي، و ممدوح محمد الجنهبي. (2006). أمن المعلومات الالكترونية. مصر: دار الفكر الجامعي.

● قائمة المراجع باللغة الانجليزية:

- Huang, & al. (2010). Perception of information security. London.
- Jacobs, S. (2011). *Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance*. Canada: Prentice Hall.
- Siponen, B., & Baskerville, J. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management* , 319-367.
- Veiga, D., & Eloff. (2010). A framework and assessment instrument for information security culture. U.S.A.

● قائمة المراجع باللغة الفرنسية:

- Benjamin, A. (2009). *Normes Iso 27001/ Iso 27002: principes de base et aspects techniques, guides de consultation en sécurité informatique*. France: Hervé schauer consultant Ed.
- Claude, B. B., & Possin, J. (2006). *De l'intelligence des risques à la mission de protection*. France: Ed IFIE.
- Henry Bouchet, M. (2007). *L'Intelligence Economique et Gestion des risques*. France: Ed Pearson Education.
- Jakobiak, F. (2004). *L'intelligence Economique: la comprendre, l'implanter, l'utiliser*. France: Ed d'organisation.
- Laurent, C., & Wolfhugel, B. (2011). *Sécurité informatique: principes et méthodes*. France: Ed Eyrolles.