أثر تكنولوجيا المعلومات على الأمن المعلوماتي

The impact of information technology on information security)

لرقط سمية، جامعة محمد خيضر بسكرة ، slarguet@escf-constantine.dz

معاليم سعاد، جامعة محمد خيضر بسكرة ، souad.malim@univ-biskra.dz

تاريخ الاستلام: 2021/03/22 تاريخ القبول: 2021/07/04 تاريخ النشر: 2021/12/31

ملخص: نظرا لما تمتاز به تكنولوجيا الحديثة من دقة وسرعة في نقل المعلومات وتبادلها دون النظر إلى الحدود الجغرافية والزمنية أصبحت أغلب المؤسسات تعتمد عليها في تسير أعمالها. يهدف هذا البحث لتحديد علاقة التكنولوجيا بالأمن المعلوماتي، إبراز الآثار السلبية والإيجابية لها عليه والتدابير اللازمة لحماية المعلومات وذلك من خلال الاعتماد على المنهج الوصفي التحليلي في سرد الواقع وتحليله، مع دراسة حالة لبحث مدى كفاية جهود حماية الأمن المعلوماتي في ظل مخاطر تكنولوجيا المعلومات. حيث تم التوصل إلى أنه لتكنولوجيا المعلومات رغم أهميتها العديد من المخاطر على الأمن المعلوماتي.

الكلمات المفتاحية: تكنولوجيا المعلومات؛ الأمن المعلوماتي؛ الجرائم الالكترونية.

تصنيف JEL : *XN2،XN1*

***Abstract*:**
Due to the accuracy and speed of modern technology in transferring and exchanging information without considering geographical and temporal boundaries, most institutions have become dependent on them in the conduct of their business. This research aims to determine the relationship of technology with information security, highlighting the negative and positive effects it has on it, and the measures necessary to protect information by relying on the descriptive and analytical approach in narrating and analyzing reality, and the inductive approach

.**keyword**: information technology; information security; cybercrime.
JEL classification code :*XN1, XN2*

***المؤلف المرسل*: لرقط سمية،**

***الإيميل*: larkhat.soumia@yahoo.fr**

1. مقدمة:

نظرا لما تمتاز به تكنولوجيا المعلومات الحديثة من دقة وسرعة في نقل المعلومات وتبادلها دون النظر إلى الحدود الجغرافية والزمنية أصبحت أغلب المؤسسات تعتمد عليها في تسير أعمالها، إلا أن هذه المكاسب المتطورة لم تمنع من وجود تأثيرات سلبية لها على الأمن المعلوماتي وحمايته، وذلك لأن تقنياتها العالية والمتطورة سلاح ذو حدين، فقد منحت القدرة على الاختراق و الاعتداء على خصوصية المعلومات أيا كان نوعها للأفراد والمؤسسات من خلال ما يسمى بالجرم المعلوماتي، و ساعدت على ارتكاب جرائم إلكترونية يصعب اكتشافها والتعرف على هوية مرتكبها ووقت ارتكابها، بالنظر إلى عدم وجود الأدلة المادية التي تكشفه، وهذا ما أصبح يشكل خطرا على الأمن المعلوماتي لأي جهة أو مؤسسة أو حتى خصوصية الأفراد. ولهذا أصبحت حماية الأمن المعلوماتي للشركات في كل دول العالم مطلبا أساسيا في وقتنا الحالي، وانطلاقا مما سبق يمكن طرح السؤال الرئيسي الآتي:

إلى أي مدى يمكن أن تؤثر التكنولوجيا المعلومات على الأمن المعلوماتي للشركات الاقتصادية في الجزائر؟

يندرج تحت هذا السؤال الأسئلة الفرعية التالية:

- ما هي المخاطر المحتملة لاستخدام تكنولوجيا المعلومات على الأمن المعلوماتي؟
- ماهي الاستراتيجية التي تعتمد عليها الشركة لحماية أمنها المعلوماتي؟
- هل الإجراءات المتبعة من طرف شركة عين الكبيرة لصناعة الاسمنت كافية لحماية أمنها المعلوماتي؟

وتتمثل أهداف هذا البحث فيما يلي:

- تحديد علاقة التكنولوجيا بالأمن المعلوماتي، والتطرق للتأثيرات الايجابية للتكنولوجيا على الأمن المعلوماتي وكيفية الاستفادة منها لخدمة الأفراد والمؤسسات.
- التطرق للآثار السلبية الخطيرة التي أفرزتها التكنولوجيا على الأمن المعلوماتي، وتحديد التدابير اللازمة لحماية المعلومات والحفاظ على سريتها وسلامتها.
- تقييم الاستراتيجية التي تعتمد عليها الشركة محل الدراسة في حماية أمنها المعلوماتي، وتحديد إذا ما كانت الإجراءات المتبعة كافية لتحقيق ذلك.

سنحاول الإجابة على الإشكالية والأسئلة المطروحة من خلال المحاور الموالية:

2. المحور الأول: تكنولوجيا المعلومات والأمن المعلوماتي

تتطلب الدراسة التي نتناولها ضرورة الوقوف على العناصر الأساسية لكل من الأمن المعلوماتي والتكنولوجيا، من حيث تعريفهما وتحديد العلاقة التي تربط بينهما.

1.2. تعريف الأمن المعلوماتي:

وضعت تعريفات عدة للأمن المعلوماتي ترتبط بالزاوية التي يدرس منها، من تعريفاته:

الأمن المعلوماتي هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها من أنشطة الاعتداء عليها، ومن الناحية التقنية هو مجموع الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية و الخارجية، أما من زاوية قانونية الأمن المعلوماتي هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو غرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف نظمها (جرائم الكمبيوتر والانترنت). (المدادحة، 2011، صفحة 109)

وعليه يمكن القول إن مفهوم الأمن المعلوماتي يشمل النقاط الآتية:

– حماية المعلومات من الضرر بكل أشكاله، وأيا كان مصدره (أشخاص كالمخترقين أم برامج كفيروسات الحاسوب)، وسواء كان متعمدا أم عن طريق الخطأ.

– حماية المعلومات من الوصول غير المصرح به، أو السرقة، أو الالتقاط، أو التغيير، أو إعادة التوجيه، أو سوء الاستخدام.

– حماية قدرة المؤسسة على الاستمرار وأداء أعمالها على أكمل وجه.

– تمكين أنظمة تقنية المعلومات و البرامج التطبيقية لدى المؤسسة من العمل بشكل آمن. (القحطاني، 2015، صفحة 58)

2.2. تعريف التكنولوجيا:

تطور المعنى الفعلي للتكنولوجيا على مر العصور إلى أن وصلت إلى ما نشهده حاليا من تقدم تكنولوجي كبير نكاد لا ندركه أحيانا، فقد أصبحت التقنيات والتكنولوجيا الحديثة تدخل في مجالات الحياة كلها، من هواتف وحواسيب وأجهزة إلكترونية متطورة.. وأصبحت كل المؤسسات الصناعية والاقتصادية والعسكرية وغيرها تعتمد بشكل أساسي على التكنولوجيا المتطورة في تسيير شؤونها وتقديم خدماتها.

وبما أننا نتكلم عن الأمن المعلوماتي وأثر التكنولوجيا المعاصرة عليه، فإن التكنولوجيا التي نحاول توضيح معناها هي تكنولوجيا المعلومات، والتي يقصد بها مجموعة من التقنيات والأدوات والوسائل أو النظم المختلفة التي يتم توظيفها لمعالجة المضمون أو المحتوى الاتصالي الذي يراد توصيله من خلال عملية الاتصال الجماهيري أو الشخصي أو التنظيمي، والتي يتم من خلالها جمع المعلومات والبيانات المسموعة أو المكتوبة أو الرقمية في الحاسبات الإلكترونية حسب مرحلة التطور التاريخي لوسائل الاتصال. (مغيزلي، 2018، صفحة 172)

3.2. علاقة التكنولوجيا بالأمن المعلوماتي:

وباعتبار الانترنت الرابط الجوهري لوجود علاقة بين التكنولوجيا والأمن المعلوماتي، تتيح العولمة المعلومات والاتصالات دون أي اعتبار للحدود الجغرافية، وهذا الأمر يعتبر أخطر قضايا العصر التي تتعلق بإدارة المعلومات، لأن إتاحة المعلومة تهدف بالدرجة الأولى إلى الاقتصاد في الجهد والوقت والتكلفة من أجل تعظيم كفاءة وفعالية المؤسسات. وبالتالي هناك ضرورة حتمية لحماية خصوصية الأفراد في طلبهم واستخدامهم للمعلومات، وكذا الزامية تحديد مستويات الأمن التي يتطلبها الأمر، من أجل تحقيق الخصوصية.

فالتكنولوجيا المعاصرة ساهمت في زيادة الترابط بين العالم، و زيادة الاعتمادية بين المؤسسات المالية، و الأعمال، و المنظمات و الدول و الشعوب مما أضاف أنواع جديدة من المخاطر الأمنية تهدد مصالح الجميع دون تمييز، فانتشار فيروس مثلا على الشبكة يهدد جميع مستخدميها من كل الدول دون استثناء. (البداينة، 2006، صفحة 17، 18) كما يساهم نقص التدريب والتوعية الملائمة على أمن المعلومات في ظل وجود التكنولوجيا في جهل الكثير من العاملين والمستخدمين بالأضرار الناتجة من سوء استخدام المعلوماتية، وقد لا تستخدم أيا من مقاييس الأمن حتى البدائية منها، مما يؤدي إلى آثار تعود بالسلب والإساءة لأمن المعلومات. (الشلبي، 2009، صفحة 227)

وهذا ما يجعل أمن وسرية المعلومات الشخصية بالذات مشكلة كبرى في ظل ثورة الاتصالات وتكنولوجيا المعلومات، فعلى الرغم من أن الاعتداء على البيانات الإلكترونية قد يكون بصفة عرضية أو أمرا متعمدا (الهوش و محيريق، 2011، صفحة 241)، إلا أن الأمن المعلوماتي يحتاج إلى توفير الوسائل والإجراءات الفعالة التي تحقق الحماية الكافية من

التهديدات التي تؤدي عادة إلى فقد إحدى جزئيات نظام أمن المعلومات وبياناته ويتم الاطلاع على خصوصيتها واستخراجها بطرق غير مشروعة لاستغلالها.

وبذلك فإن التكنولوجيا مكنت من إعطاء نوع من الخصوصية لحماية البيانات التي تعد العنصر الأول في تحقيق الأمن المعلوماتي، وبدونها لا تكون هناك أي أهمية لوجود الأمن المعلوماتي وضرورة توفير حماية له من مخاطر التكنولوجيا المتطورة، باستخدام جهاز إلكتروني مصمم خصيصا لاستقبال المجاميع الكبيرة من البيانات بشكل آلي وتخزينها، ومن ثم إمكانية تحويلها إلى نتائج ومعلومات مفيدة يمكن استخدامها حسب الحاجة وعند الطلب بموجب أوامر وتعليمات خاصة يطلق عليها برامج التشغيل (ياسع، 2011، صفحة 41)، وهي تستند في ذلك على البرمجيات الموثقة والمدعمة بأدلة إرشادية للتشغيل، والتي تعد من أهم أجزاء ومكونات الحاسوب وأكثرها أرباحا بالنسبة للعاملين في مجال إنتاجها وتسويقها وكان لها الأثر المباشر في ظهور مصطلح "صناعة المعلومات". (الدلاهمة، 2007، صفحة 364)

3. المحور الثاني: مظاهر تأثير التكنولوجيا على الأمن المعلوماتي

تتعدد المظاهر التي تتجلى فيها تأثيرات التكنولوجيا على الأمن المعلوماتي بين ما هو إيجابي وما هو سلبي، وأهمها ما يلي:

1.3. الإيجابيات: (الدلاهمة، 2007، صفحة 61)

أ.التواصل عن بعد: تتيح تكنولوجيا المعلومات إمكانية التواصل بين المستخدمين في مواقع مختلفة بفضل شبكة الانترنت، واستخدام نظم وبرامج التشغيل المتعددة ما يسمح بتدفق المعلومات بكل سهولة وبتكاليف منخفضة، كما تسهل العلاقة مع شركاء الأعمال داخل أي منظمة وخارجها من أجل زيادة إنتاجية الخدمة وتطويرها بشكل أسرع، باستخدام وسائل التواصل الالكترونية التي نذكر منها: البريد الإلكتروني، المواقع الإلكترونية.

ب. العمل التجاري الإلكتروني: من الخدمات المتطورة التي أصبحت تقدمها التكنولوجيا، العمل الإلكتروني الذي يقوم على إجراء المعاملات والصفقات التجارية عبر الوسائل الإلكترونية الحديثة، من خلال شبكات المعلومات، مما يساعد على الاقتصاد في التكاليف وتقليص المسافة بين المنتج والمستهلك. (البشكاني، 2009، صفحة 50)

ج. تطوير تقنيات الأعمال المالية والمصرفية: تعد الأعمال المالية والمصرفية من أساسيات دعم تكنولوجيا المعلومات، وأصبحت الخدمات المالية والمصرفية تعتمد على النقل الإلكتروني للأموال وبطاقات الائتمان والصكوك الإلكترونية بين مختلف المتعاملين ، وذلك لتوفير الوقت والسرعة في الأداء والوفاء المالي. (البشكاني، 2009، صفحة 61)

د. استرجاع ونقل المعلومات عبر الانترنت: أصبح بالإمكان تناقل الملفات عن بعد، بشرط أن تعرف الموقع الدقيق للحواسيب التي تضم الملفات، أو بالأحرى مواقع الملفات المخزنة في تلك الحواسيب، إذ بالإمكان الدخول والبحث عن الملف المطلوب، تحديد موقعه، استرجاعه ونقله بكل سهولة. (ياسع، 2011، صفحة 70)

هـ. تنظيم تبادل المعلومات والخدمات الإدارية: يعتمد في ذلك على وجود نماذج معيارية متفق عليها بدلا من استخدام البريد العادي، لذا يمكن للشركة أو المؤسسة أن تستغني على معظم المعاملات الورقية التي تقدم التكنولوجيا المتطورة حلولا جذرية بديلة عنها، لحفظ تلك المعلومات والبيانات بشكل آلي في جهاز الخادم الآلي للبريد الإلكتروني وغير ذلك من وسائل التخزين الإلكترونية.

2.3. آثار سلبية:

أ. **القرصنة الإلكترونية:** تعتبر من الآثار السلبية للتكنولوجيا وهي عبارة عن دخول إلى نظام التشغيل في أجهزة المستخدمين الآخرين بطرق غير مشروعة، لأغراض غير مشروعة كالسرقة والتخريب استنادا إلى نقل أو مسح الملفات أو إضافة ملفات أخرى وبرامج وهمية، ويستغل القراصنة نقاط الضعف في الحواسب الضعف في الحواسب الأمنية لمواقع الشبكة العنكبوتية، للحصول على معلومات وبيانات خاصة بالزبائن. (البداينة، 2006، صفحة 177)

من أجل الحد من تزايد عمليات التسلل والقرصنة، اضطر مسؤولو أمن الحواسيب والشبكات ورجال الأمن للاستعانة بخبرات بعض المحترفين في التسلل ليستطيعوا تطوير نظم الحماية ضد المتسللين، ومثال ذلك يرسل مستولي أمن المعلومات أسئلة تتعلق بأحدث سبل الحماية لغرف الدردشة الخاصة بمواقع غرفة المتسللين، أو ما يعرف باسم(hacker internet chat room)، لطلب آراء ونصائح تقنية حول أحدث سبل الحماية من التسلل. (الهوش و محيريق، 2011، صفحة 186)

ب. **الخداع وانتحال الشخصية:** تتطلب عملية الاعتداء على الأمن المعلوماتي أحيانا اللجوء إلى أسلوب الخداع، بتقديم بعض الأشخاص لأنفسهم إلى الآخرين على أنهم ممثلين لشركات وواضعين مواقع وهمية على الويب يستطيعون من خلالها جمع معلومات سرية، مما يؤدي إلى تضليل الشخص المستقبل للمعلومات حيث تبدوا أنها مرسلة من جهة معينة، وتكون في واقع الأمر مرسلة من جهة أخرى.(الهوش و محيريق، 2011، صفحة 233)

ج. **الاعتداء على المعطيات:** يكون الغرض منها الدخول على المعطيات السرية والمحمية أو الخصوصية الشخصية وعلى البيانات التي لها صفة بالحياة الفردية، من خلال استخدام الانترنت من أجل التزوير أو الاختلاس ، وهذا ما يترتب عليه تجسس على الحياة الخاصة والاطلاع على حياة الأشخاص وخصوصياتهم من دون علمهم بذلك ودون إذنهم، وغالبا ما تتم عمليات التجسس باستخدام نوع من الفيروسات التي تنقل إلى الحواسب وتعمل على إرسال نسخ من البيانات والمعلومات إلى حاسوب آخر، أو تمكينه من التجسس الرقمي. (الشلبي، 2009، صفحة 169)

د. **النصب في مجال الخدمات الالكترونية:** يعتبر النصب وسرقة المال المعلوماتي في مجال المنتجات والخدمات التجارية التي تقدمها الشبكة العنكبوتية بوسائل غير مسبوقة إحدى أهم الأساليب التي يعتمد عليها الجاني في احتياله على الأمن المعلوماتي للأشخاص أو الشركات والمؤسسات، كاستخدام البريد الالكتروني أو عرضها على مواقع على الشبكة واستخدامها بطرق غير قانونية بعيدا عن تناول يد غير المصرح لهم بالنسخ غير القانوني للبيانات وقرصنة برمجيات الحاسب كما تقوم هذه العملية بناء على طلب الشخص المحتال من الضحية عبر الانترنت بحدوث خلل في البيانات في الحساب البنكي مثلا، يستلزم ذلك بسرعة إعادة إدخال بيانات جديدة من اسم الضحية وتاريخ ميلاده العنوان ورقم الحساب حتى تتم معاملاته البنكية. (البداينة، 2006، صفحة 227)

ومثال الجرائم المالية من السهولة الحصول على أرقام بطاقات الائتمان من الانترنت، حيث قامت بعض مواقع الشبكات بعرض قوائم تحتوي على أكثر من (25000) رقم بطاقة ائتمان حصلت عليها من سبعة مواقع للتجارة الكترونية باستخدام قواعد وبيانات متوفرة تجاريا، ولم يمكن ليصعب على أي متطفل استخدام ذات الوسيلة البدائية للاستيلاء على أرقام

البطاقات واستخدامها في عمليات شراء يدفع قيمتها أصحابها الحقيقيين. (الهوش و محيريق، 2011، صفحة 187)

هـ. **الفيروسات:** تعتبر الفيروسات من الأساليب التي يتم الاعتداء بها على المعلومات، وهي برامج حاسوب مكتوبة لإلحاق الضرر بأجهزة وبرامج الحاسب، وبالنسبة للفيروسات التي تأثر على المعلومات والبيات تقسم الى نوعين، منها فيروس الماكرو (macro virus)، وهو عبارة عن برنامج صغير مكتوب باستخدام برمجة داخلية للتطبيقات يقوم هذا الفيروس على عمل نسخ من نفسه بداخل الملفات المنشاة باستخدام البرامج التطبيقية مثل معالج النصوص، يعمل بمجرد فتح الملف أو إغلاقه أو عند حفظه، أما فيروس قطاع التشغيل(boot sector virus)، يرتكز في قطاع التشغيل لأقراص الحاسوب ولا يحتاج إلى ملفات للدخول إلى جهاز لحاسوب، حيث يصاب الجهاز بالفيروس إلى الذاكرة ويحدث عدوى لكل قرص يتم تشغيله على الجهاز. (الهوش و محيريق، 2011، صفحة 231)

ومما يلاحظ فإن أهم السمات التي تميز العصر الذي نعيشه هو ازدياد استخدامات المعلومات من حولنا خاصة مع ما وفرته تكنولوجيا الانترنت من سهولة في الحصول عليها، والاطلاع عليها في أي وقت بالاعتماد على البريد الإلكتروني وتزايد المواقع التي تسهل من تقديم خدماتها على الشبكة العالمية، والاحتفاظ بها في الحاسوب الشخصي للمتصفح، وبالتالي تتطلب حماية هذه الاستخدامات للمعلومات والبيانات المدونة إلكترونيا، توفير نوع من الحماية للمعلومة الإلكترونية من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، بالاعتماد على الوسائل والإجراءات اللازمة، من خلال الأمن المعلوماتي الذي يعد وسيلة فعالة في التصدي لأي اعتداء على المعلومة الإلكترونية.

4. المحور الثالث: دراسة تحليلية بمؤسسة صناعة الاسمنت لعين الكبيرة [1]

1.4. التعريف بالمؤسسة محل الدراسة:

شركة الاسمنت لعين الكبيرة"**SCAEK**" هي شركة مساهمة عمومية (**SPA**) برأس مال قدره **2 200 000 000.00** دج، و هي فرع من الفروع الاثنين والعشرين (22) للمجمع الصناعي والتجاري لمؤسسات الاسمنت الجزائرية **GICA** الذي تأسس سنة 2010، والتي تقوم بعدة أنشطة منها إنتاج الاسمنت، إنتاج الحصى، الصيانة، التكوين، القيام بالدراسات، التسويق ...الخ. ومن أهم **المراحل التي مرت بها الشركة:**

- **1974:** انطلقت عملية إنجاز المصنع من طرف الشركة الألمانية **KHD**، أما عن بداية الدخول الفعلي للمصنع في الإنتاج فقد بدأ في شهر نوفمبر 1978 بطاقة إنتاجية قدرها مليون طن سنويا، ولم يحقق المصنع هذه النتيجة إلا سنة **2000**.
- **1998:** انفصال الشركة عن باقي وحدات صناعة الاسمنت الوطنية و ميلاد شركة الاسمنت بعين الكبيرة **SCAEK** التي تقوم بإنتاج و تسويق مادة الاسمنت و التابعة للمجمع الصناعي و التجاري للإسمنت و مشتقاته – شرق **GIC-ERCE**.
- **2002:** تحصلت على شهادة نظام الجودة بموجب معيار 9001 **ISO** نسخة 2000.
- **2005:** تم إمضاء عقد مع **ICER** من أجل تزويد ورشات الإنتاج بنظام تشغيل آلي.
- **2006:** في شهر ماي تم تركيب المصفاة الأنبوبية التي تقوم بمعالجة غاز تسخين الفرن، وقد استعملت هذه التقنية لأول مرة في الجزائر من طرف **SCAEK**.
- **2008:** في شهر جوان تم الحصول على شهادة 14001 **ISO** نسخة 2004، وعلى شهادة 9001 **ISO** نسخة 2008، كما تحصلت على الجائزة الوطنية الثانية للمحافظة على المحيط من طرف وزير تهيئة المحيط والبيئة.
- **2010:** تم إعادة هيكلة الشركة بعد إنشاء مجمع **GICA** وتحويل الأسهم والحصص الاجتماعية والمساهمات ومختلف القيم المتداولة، والممتلكة من طرف مجمع **ERCE** المصفى لحساب مجمع **GICA** و**هذا** ابتداء من تاريخ 30 مارس 2010، بالإضافة إلى الحصول على شهادة 14001 **ISO** نسخة 2008.
- **2011:** تم تجاوز سقف 1022040 طن من مادة الكلنكار لأول مرة في تاريخ الشركة، كما تم الحصول على شهادة 18000 **OHSAS** نسخة 2007 والمتعلقة بالصحة والسلامة المهنية.
- **2014:** اتخاذ توصية إدخال الشركة في البورصة وتم الانتهاء من اجراءات الدخول بتاريخ 13 جوان 2016، وانطلاق أشغال انجاز خط الإنتاج الثاني.
- **2017:** دخول خط الإنتاج الثاني حيز الخدمة.

2.4 منهجية الدراسة:

تم الاعتماد على المنهج الوصفي التحليلي في سرد وتحليل واقع علاقة التكنولوجيا بالأمن المعلوماتي، مع إبراز الآثار السلبية والإيجابية لها عليه والتدابير اللازمة لحماية المعلومات،

كما اعتمد على دراسة حالة في الجانب التطبيقي للتطرق لأهم المخاطر التي تواجه الشركة الاقتصادية الجزائرية وتقييم استراتيجيتها في حماية أمنها المعلوماتي، وتم استخدام أداة المقابلة في جمع المعلومات، حيث تمت مع المدير المالي والمحاسبي، مسؤول دائرة الأمن المعلوماتي ومدير التكوين.

-

- **3.4 أهم التهديدات والمخاطر التي تواجهها الشركة:**

تتعدد التهديدات التي يمكن أن تمس الأمن المعلوماتي ويكمن تقسيمها الى ثلاث فئات رئيسية هي:

أ. تهديدات فنية: وهي ناجمة عن القصور والأخطاء الفنية في مختلف أنظمة أمن المعلومات، والتي يغلب عليها الطابع الفني، دون أن يكون هناك أي تدخل بشري، أو أن تكون بسبب كارثة طبيعية، ومنها:

- تهديدات عيوب التصميم والتشغيل: وتشمل عيوب التصميم في الأجهزة والبرامج والشبكات وأدوات الربط والتخزين، أو أي مكون آخر من مكونات الأنظمة المعلوماتية، وهنا تبرز أهمية تصميم البنية التحتية لتقنية المعلومات وأمن المعلومات، كالبنية التحتية لخوارزميات التشفير ومفاتيحه. ولا تقل أخطار عيوب التشغيل عن أخطار عيوب التصميم في إمكانية النفوذ الى المعلومات بصفة غير شرعية، أو التسبب في فقدها بسبب خطأ تشغيلي قد يكون بسيطا.
- تهديد تشتت المعلومات: إذا كانت معلومات المؤسسة مشتتة ومخزنة في أماكن كثيرة، ويجري التعامل معها من خلال شبكات متعددة، فان هذا يتسبب في ضعف منظومة أمن المعلومات وتشتتها، وكذلك زيادة تكاليف توفيرها وادارتها والسيطرة عليها. (القحطاني، 2015، صفحة 61، 62)

ب. تهديدات بشرية: يقصد بها التهديدات الناجمة عن العنصر البشري مباشرة سواء كان عمدا أو عن طريق الخطأ، حيث يتسبب في الحاق الضرر بالمعلومات أو الوصول اليها والاطلاع عليها دون أن يكون له صلاحية ذلك، أو اتلافها أو تسريبها الى جهات خارجية. وتزداد الخطورة عندما يكون لدى هذا العنصر صلاحية الدخول الى أنظمة

المعلومات، أو يكون أحد موظفي المؤسسة، ويسيء استخدام صلاحياته. (القحطاني، 2015، صفحة 62)

ج. تهديدات طبيعية: يقصد بها الكوارث الطبيعية التي لا دخل للإنسان أو التجهيزات الفنية في حدوثها، كالزلازل، الفيضانات، الحرائق... الخ، حيث تسبب أضرارا كبيرة لأنظمة المعلومات، ويمكن أن تصل الى توقف الخدمات الالكترونية نهائيا (القحطاني، 2015، صفحة 63)

تتمثل أهم المخاطر التي تواجه الأمن المعلوماتي للشركة في خطرين أساسين هما:

- العامل البشري خاصة فيما يتعلق بتسريب المعلومات خارج الشركة عن قصد أو عن غير قصد،
- الاتصال بشبكة الانترنت وما يصاحبها من مخاطر، خاصة فيما يتعلق بالجانب المالي لاعتمادها على الدفع الالكتروني لتسديد التزاماتها خاصة مع مصالح الضرائب منذ عشر سنوات، وتجدر الاشارة الى ان هذا الخطر ليس متعلق بإجراءات المؤسسة في الحماية بل بالأطراف المتعامل معها.

4.4. آليات تحقيق الأمن المعلوماتي لشركة صناعة الاسمنت بعين الكبيرة:

تقوم آليات تحقيق الأمن المعلوماتي على اتخاذ جملة من الإجراءات والتدابير اللازمة لحماية المعلومات من التغيير والحفاظ على سريتها وسلامتها من أي اعتداء ناتج عن تأثير تكنولوجيا المعلومات. حيث كلما كانت هناك إجراءات أكثر تفصيلا ودقة كانت معرفة المخالفات أسهل، وكلما كانت القواعد مكتوبة ورسمية كان فرضها ومتابعتها أسهل. لذا يجب أن يشتمل برنامج أمن المعلومات على: السياسة الأمنية والتي تشكل الأساس الذي يتم بناء البرنامج عليه، والمعايير القياسية، الخطوط الأساسية، المبادئ التوجيهية والإجراءات، وبرامج التوعية المنظمة لأمن المعلومات التي تمثل إطار العمل لهذا البرنامج.

أ. **السياسة الأمنية:** تعتبر حجر الزاوية للتخطيط لأمن المعلومات، وهي الوثيقة الرسمية للمؤسسة التي تصدرها الإدارة العليا، تتضمن كيفية أداء الأعمال ذات العلاقة بأمن المعلومات وكيفية معالجة أي نشاط يخص المعلومة أو الأنظمة والأشخاص المعالجين لها. (القحطاني، 2015، صفحة 185، 186) وتشمل:

– **السياسة الأمنية العامة:** التي تحدد برنامج أمن المعلومات وأهدافه والآليات والطرق التي تضمن فرضه وتطبيقه على أرض الواقع، والمسؤوليات اللازمة لتنفيذه.

– السياسة الموضوعية المتخصصة في موضوعات أو تخصصات معينة بشكل تفصيلي أكثر من السياسة الأمنية العامة.

– السياسة الأمنية الخاصة بأنظمة محددة كتلك الخاصة بتنفيذ قرارات الإدارة المتعلقة بأنظمة تقنية المعلومات المستخدمة فيها كالبرامج التطبيقية، والشبكات. (القحطاني، 2015، صفحة 210)

وتحديد السياسة الأمنية للمؤسسة له أهمية كبيرة يمكن تلخيصها في النقاط التالية:

- تحديد أهداف المؤسسة المتعلقة بأمن المعلومات،
- تحديد أهم موارد المؤسسة والمعنية بالحماية،
- تسهيل عمل فريق أمن المعلومات، وتحدد نطاق عمله ومهامه.
- تمثل مرجعية رئيسية وموحدة لكل الأطراف داخل المؤسسة خاصة عند تعارض المهام الخاصة بأمن المعلومات، أو عدم تطبيقها.
- تحدد وتوضح مسؤوليات الموظفين المتعلقة بأمن المعلومات.
- تساهم في منع حدوث مفاجآت في الاجراءات او الطلبات أو الأحداث اليومية. (القحطاني، 2015، صفحة 188)

ب. المعايير القياسية: هي الأنشطة والأعمال واللوائح الإلزامية التي يتقيد بها في جميع أنشطة المؤسسة، وهي تدعم السياسات الأمنية وتجعلها تأخذ صفة القطعية والزامية التنفيذ. قد تكون داخلية المنشأ والتطبيق أي خاصة بالمؤسسة، وقد تكون خارجية المنشأ ويفرض عليها تطبيقها مثل المعايير الحكومية. من أمثلة المعايير نذكر:

– إلزام الموظفين بتشفير البيانات السرية داخل المؤسسة، وأي بيانات تحزن على الأجهزة المحمولة.

– إلزام الموظفين باستخدام الخصائص الحيوية كبصمة الأصابع للتحقق من هوياتهم عند الدخول للأنظمة عالية الحساسية.

ج. الخط الأساسي: هو المستوى الأدنى من الحماية المطلوبة والذي يجب المحافظة عليه عند وقوع أي خطر أو اجراء أي تغيير في المؤسسة، ويعد المرجع الذي يقاس به مدى قرب

أو بعد وقوع الخطر، بحيث يجب المحافظة دائما على البقاء فوق الخط الأساسي للحماية. كما يجب تطبيق هذا المفهوم في المؤسسة ومراجعة هذا الخط بعد اجراء أي تعديل تفاديا لحدوث أي ثغرات أمنية.

د. **التوجيهات:** إرشادات عامة غير الزامية موجهة للمستخدمين والمختصين في تقنية المعلومات، وتشمل طرق الاستخدام للتقنيات المتاحة في المؤسسة، ويرجع لها في حال وجود غموض في السياسات الأمنية أو المعايير أو الإجراءات للحصول على معلومات أكثر تفصيلا.

ز. **الاجراءات:** هي الخطوات التفصيلية المطلوب القيام بها لتحقيق هدف معين، حيث تحدد كيفية تطبيق السياسات الأمنية والمعايير القياسية والتوجيهات على أرض الواقع، نذكر منها مثلا:

– الخطوات التفصيلية لتغيير اعدادات أنظمة الحماية وآلياتها،

– الخطوات التفصيلية لمنح الصلاحيات على الأجهزة.

يمكن القول إذا أن السياسة الأمنية هي بمثابة هدف استراتيجي للمؤسسة يجب تحقيقه، والمعايير القياسية والتوجيهات والإجراءات هي بمثابة الوسائل والمكونات الداعمة لتحقيق ذلك الهدف. (القحطاني، 2015، صفحة 199، 200، 201)

و. **التدريب والتوعية بأمن المعلومات:** الهدف منه هو إيصال مفهوم أمن المعلومات والسياسة الأمنية لكل موظفي المؤسسة، والتأكد من أن المعايير القياسية والإجراءات والتوجيهات قد وصلت بالصورة الصحيحة لكل شخص يتطلب عمله فهمها وتطبيقها والتعامل معها. وبهذه الطريقة يمكن تحديد من يحتاج الى التدريب أو التوعية وفي أي مجال. ويشتمل كل من التدريب والتوعية بأمن المعلومات على ثلاث مستويات:

– **المستوى الأعلى:** وهو مستوى عام وشامل يحتوي على مواد تدريبية وتوعوية، قصيرة المدة، عامة المفاهيم، لمعرفة الخطوط العريضة لكل من السياسات الأمنية والمعايير القياسية والتوجيهات والاجراءات، دون التطرق للتفاصيل، وهو موجه للمستويات العليا من الادارة.

– **المستوى المتوسط:** متوسط الشمولية، ويحتوي على مواد تدريبية وتوعوية متوسطة المدة ومتوسطة التفاصيل، وهو موجه للمهندسين والاستشاريين ورؤساء الأقسام.

– **المستوى الادنى:** هو مستوى تفصيلي يحتوي مواد تدريبية وتوعوية طويلة المدة، تحتوي معلومات تفصيلية عن كيفية تطبيق السياسات الامنية، والمعايير القياسية، والتوجيهات، والاجراءات خطوة بخطوة على أرض الواقع، وهو موجه للأفراد والجهات التنفيذية.

يجب أن يكون التدريب والتوعية بأمن المعلومات مستمرين طوال العام، وبصفة دورية، وأن يشمل كل المستويات مرة واحد على الأقل سنويا. (القحطاني، 2015، صفحة 209)

5.4 استراتيجية حماية الأمن المعلوماتي لشركة صناعة الاسمنت بعين الكبيرة:

1. تعتمد الشركة سياسة لحماية أمنها المعلوماتي لكنها غير موثقة وغير مكتوبة، الا فيما يخص بعض العناصر المتعلقة بإجراءات التسيير من خلال نظام الجودة الا أنه لا يغطي كل جوانب المعلومات. وهو موثق في التعليمة رقم 001/900 وتتعلق بنسخ قاعدة البيانات.
2. يتم تحليل المخاطر وخطة الأمن المعلوماتي المعتمدة من فترة إلى أخرى عادة كل شهر ولكن في إطار نظام الجودة والتدقيق الداخلي الذي يشمل جانب فقط من المعلومات غير موثقة.
3. يتم اطلاع الموظفين على السياسة الأمنية للشركة وتعريفهم بواجباتهم لكن فيما يخص عمال دائرة الأمن المعلوماتي فقط وليس كل العمال، ويتعلق الأمر دائما بنظام الجودة.
4. لا يتم تدريب الموظفين على مسائل الأمن المعلوماتي الا من ينتمون الى دائرة الأمن المعلوماتي الذين يخضعون لتدريب خارجي وآخر داخلي، لكن تم اجراء حلمة تحسيسية من طرف مختص في القانون لتعريف العمال بوجوب سرية المعلومات الداخلية وعدم التصريح بها او نقلها لخارج الشركة.
5. أما فيما يخص الموظفون الجدد فلا يتم تدريبهم ولا تعريفهم بمحتوى الخطة المتبعة لحماية الأمن المعلوماتي الا من سيعينون في دائرة الأمن المعلوماتي.
6. كما أنه لا يتم فحص تأهيل وكفاءة ومدى التزام الموظفين بتحقيق معايير الأمن المعلوماتي(قبل التوظيف، أثناء فترة التوظيف، بعد انتهاء خدمتهم).
7. كما أنه لا تتوفر نصوص في العقود مع الموظفين تحدد وتصف بدقة واجباتهم الوظيفية المتصلة بالأمن المعلوماتي للشركة (نصوص تحكم العلاقة أثناء وبعد انتهاء الخدمة) فيما يتعلق بالأمن المعلوماتي للشركة.

8. فيما يتعلق بالبرمجيات تعتمد الشركة على سياسة خاصة في شرائها واستخدامها وكذا الرخص المتعلقة بها، حيث تعتمد على برامج داخلية (برمجة داخل الشركة) وبرامج معتمد يتم اقتناءها بعد فترة تدريب وتكون مرخصة.
9. تعتمد الشركة على بروتوكول في تسيير الأجهزة والمعدات (من حيث الاحتياجات وتوفير المتطلبات، معايير توظيف الأجهزة في العمل، إلغاء استخدامها، مسائل الصيانة، ...الخ)، حيث تعتمد في تسيير الأجهزة عن طريق برنامج خاص**GLPI** و ذلك فيما يخص أجهزة الاستعمال الشخصي وكذا خوادم للبرامج وطابعات صناعية، ويتم بيعها بالمزاد العلني عند نهاية وقت استعمالها.
10. تتبع الشركة سياسة محددة بخصوص تخزين المعلومات وتحديد وسائط التخزين وكيفية تسييرها.
11. كما تعتمد على استراتيجية لحماية الأمن المعلوماتي للشركة من حيث توفير وسائل تحدد هوية المستخدم والتحقق من تصرفاته، التوثيق، وقت الاستخدام، وذلك بإدماجه في الشبكة الخاصة بالشركة.
12. هناك تحكم في وسائل وتطبيقات الاتصالات الداخلية والخارجية، وتوثيق حركة الاتصال مع الحفاظ على سرية استخدام البريد الالكتروني، ورصد الهجومات الخارجية باستخدام جهاز جدار ناري الذي يبرمج لتحقيق ذلك.
13. تعتمد سياسة خاصة في عملية نسخ البيانات والمعلومات، عدد النسخ المخزنة، مكان تخزينها، المكلف بعملية التخزين، استخدامها ونشرها، ويراجع ذلك دوريا.
14. تعتمد الشركة على طرق وبرامج للحد من الولوج للإنترنت من قبل الموظفين.
15. لم تتعرض الشركة لأي اختراق سابقا. تتوفر على فريق متخصص في أنظمة المعلومات والتحكم في تسييرها، ومتابعة العمل على الأجهزة والأنظمة الداخلية، لكن غير مختص في التعامل مع الحوادث والاعتداءات الالكترونية، لكنها تتوفر على أجهزة متخصصة للحماية.
16. كما أن للشركة اتصالات مع الجهات الرسمية وجهات تطبيق القانون وجهات الخبرة المتخصصة في مجال حماية أمن المعلومات من أجل المسائل المعقدة أو التي لا تتوفر كفاءات للتعامل معها داخل الشركة.

17. للشركة خطط للطوارئ في حالة الاعتداءات وخطط للتعافي، من أجل تخفيف الأضرار والعودة للوضع الطبيعي في حالة تعرض الأمن المعلوماتي للخطر.
18. تتبع الشركة سياسة خاصة من أجل توفير المعلومات التي يتعين وصولها لجهات محدد أو قطاعات معينة والتحقق من وصولها وهذا في إطار نظام الجودة من خلال عدة سبل:
ـ الإنترانت: من خلال استخدام بعض التطبيقات التي تسمح بتبادل المعلومات لكل الجهات الداخلية للشركة.
ـ الأنترنت: استخدام الايمايلات والمواقع لإرسال المعلومات داخليا وخارجيا.
ـ برنامج **FTP**: لإرسال المعلومات لمجمع **GICA**.
ـ برامج **visioconférence**: للاجتماعات.
19. الشركة أبرمت عقد تأمين مع شركة جزائرية لكن لا يشمل الأخطار الالكترونية، وانما يتعلق فقط الخسائر المادية التي يمكن أن تلحق بالأجهزة الالكترونية.

5. الخاتمة:

من خلال ما تم تناوله في هذه الورقة البحثية يمكن التوصل إلى جملة من النتائج تتمثل في:

- أن المؤسسة تهتم بحماية أمنها المعلوماتي لكن ليس بشكل كبير وهو محصور فيما يتعلق بتطبيق نظام الجودة، وهذا نظرا لمحدودية استخدامها للأنترنت في معاملاتها اليومية، والإجراءات المطبقة على استخدامه داخلها، كما انها تستخدم شبكة مغلة للتواصل فيما بينها **réseau fermé** .
- الخطر الأكبر على الأمن المعلوماتي للشركة يمكن أن يكون مصدره العامل البشري من داخلها وقد يتسبب في تسريب المعلومات، ولهذا وضعت إجراءات صارمة على استخدام وسائط نقل المعلومات، كمنع استخدام فلاش ديسك نهائيا في نقل المعلومات.
- رغم الخطر الكبير الذي تواجهه من العامل البشري الا أنها لا تحمي نفسها أثناء ابرام عقود مع العمال، وتضمين العقود بمواد تلزمهم بعدم تسريب معلومات عن المؤسسة أثناء فترة العقد أو حتى بعد انتهائه هذا من جهة،
- ومن جهة أخرى لا تخضع الموظفين الجدد – باستثناء من سيعملون في دائرة الأمن المعلوماتي – لتقييم فيما يخص مدى معرفتهم بالأمن المعلوماتي مما قد يشكل خطر عليها في حالة توظيفهم، واضرارهم بالأمن المعلوماتي لها لجهلهم بإجراءات الحماية.

- عدم اجراء تكوين دوري ولكل العمال في جانب الأمن المعلوماتي يشكل خطرا كبيرا عليها، فيمكن أن يؤدي ذلك الى التسبب بأضرار جسيمة لجهلهم بالممارسات التي تمس أمنها المعلوماتي.
- الشركة اهتمت بالجانب المادي في عقد التأمين وأغفلت الجانب المتعلق بالمعلومات.

6. التوصيات

ومن أهم التوصيات التي نقترحها لحماية الأمن المعلوماتي للشركة ومواجهة تأثيرات التكنولوجيا السلبية عليه:

- اعتماد سياسة لحماية أمنها المعلوماتي موثقة وتغطي كل جوانب الأمن المعلوماتي وليس الاكتفاء فقط بالعناصر المتعلقة بإجراءات التسيير من خلال نظام الجودة.
- اطلاع كل الموظفين على السياسة الأمنية للشركة وتعريفهم بواجباتهم وليس عمال دائرة الأمن المعلوماتي فقط.
- تأهيل العاملين في دائرة الأمن المعلوماتي في التعامل مع الحوادث والاعتداءات الالكترونية.
- اجراء تكوين دوري لكل العمال فيما يخص الأمن المعلوماتي، وبالمستوي الذي تستلزمه وظيفة كل منهم.
- إضافة بنود في العقود المبرمة مع العمال تلزمهم بسرية المعلومات أثناء فترة الخدمة وبعد انتهائها.
- مسايرة التطورات المستمرة في مجال الأساليب المتطورة لمكافحة الجرائم الإلكترونية.
- التوجه نحو ابرام عقد تأمين لتغطية الخسائر المحتملة في حال حصول أي خطر حيث يضمن هذا العقد ما يلي:
  - تغطية تكاليف إعادة تكوين قاعدة البيانات،
  - تغطية خطر الانقطاع عن العمل، حيث تدفع شركة التأمين للشركة خسارة الانقطاع عن العمل في فترة استرداد الاعمال، فترة الانتظار، فترة إعادة تكوين قاعدة البيانات،
  - تغطية تكاليف الاستجابة للطوارئ كدفع أتعاب الخبراء.

رغم أن هذا النوع من العقود لا توفره شركات التأمين الجزائرية، ولهذا يمكنها عقده مع شركات أجنبية.

7. قائمة المراجع:

[1] – المعلومات التي تخص الجانب التطبيق والمتعلقة بالشركة تم الحصول عليها من خلال اجراء مقابلة مع المدير المالي، ومدير دائرة الأمن المعلوماتي ومختص في تكنولوجيا المعلومات، ومدير التكوين بالشركة وهو أيضا مختص في تكنولوجيا المعلومات. و لمعلومات أكثر يمكن تصفح الموقع الالكتروني للشركة www.scaek.dz

2- أبو بكر محمود الهوش، و مبروكة عمر محيريق. (2011). *ادارة المعلومات* (الإصدار الطبعة 1). مصر: السحاب للنشر و التوزيع.

3- أحمد بن نافع المدادحة. (2011). *النشر الالكتروني و حماية المعلومات* (الإصدار الطبعة 1). عمان، الأردن: دار الصفاء للنشر و التوزيع.

4- ذياب البداينة. (2006). *الأمن و حرب المعلومات*. عمان: دار الشروق للنشر و التوزيع.

5- ذيب بن عائض القحطاني. (2015). *أمن المعلومات*. الرياض، المملكة العربية السعودية: مدينة الملك عبد العزيز للعلوم التقنية.

6- سليمان مصطفى الدلاهمة. (2007). *أساسيات نظم المعلومات المحاسبية و تكنولوجيا المعلومات*. عمان، الأردن: دار الوراقة للنشر و التوزيع.

7- نوال مغيزلي. (2018). تكنولوجيا الاعلام و الاتصال في الجزائر دراسة للمؤشرات و تشخيص للمعيقات. *المجلة الجزائرية للأمن و التنمية*. تاريخ الاسترداد 2021

8- هادي مسلم يونس البشكاني. (2009). *التنظيم القانوني للتجارة الاكترونية*. مصر: دار شتات للنشر و التوزيع و البرمجيات.

9- هيثم حمود الشلبي. (2009). *ادارة مخاطر الاحتيال في قطاع الاتصالات* (الإصدار الطبعة 1). عمان، الأردن: دار الصفاء انشر و التوزيع.

10- يسمينة ياسع. (2011). دراسة اقتصادية قياسية لأثر تكنولوجيا المعلومات و الاتصالات على الآداء الاقتصادي للمنظمة. *رسالة ماجستير في العلوم الاقتصادية*. بومرداس، كلية العلوم الاقتصادية و التجارية و علوم التسيير، الجزائر: جامعة أحمد بوقرة.