

الأمن المعلوماتي واختراق خصوصية المؤسسات الاقتصادية

Information security and protecting the privacy of economic institutions from digital risks

د. إيمان بن نعجة

جامعة الجزائر 3 (الجزائر)

imenebennadja@univ-alger3.dz

د. أمال بن اعراب

جامعة الجزائر 3 (الجزائر)

bnarabamel@univ-alger3.dz

ملخص:

نهدف من خلال هذه المداخلة إلى معرفة تأثير العالم الرقمي على استقرار أمن المعلومات في المؤسسة الاقتصادية، وإبراز مدى ضمان وحماية خصوصية الفرد بصفة خاصة والمؤسسات بصفة عامة. فنظرا لأهمية التكنولوجيا في وقتنا الراهن أصبح استغلالها أمرا حتميا على الأفراد والمؤسسات على حد سواء.

فالثورة الرقمية التي شهدها مجال الاتصالات والمعلومات أدت إلى العديد من المتغيرات الجديدة الخاصة بأمن المعلومات في شكلها الرقمي، وأصبحت العلاقة بالإنترنت تتطور بل وتتعدد شيئا فشيئا وصارت حياة الأفراد وأعمال المؤسسات متصلة بالإنترنت، وكل شيء متشابكًا ومعقدًا. وهنا يصبح الحفاظ على خصوصية المؤسسات أمر مهم وصعب التحكم به في آن واحد، وما زاد من تأزم الوضع انتشار المخترقين للخصوصيات، خاصة مع اشتداد المنافسة بين المؤسسات الاقتصادية، مما يدفعها لاتخاذ سبل الحيلة والحذر باتباع إجراءات الحماية اللازمة.

وبالتالي فإن تجديد نمط تفكير جميع الموظفين في المؤسسة بدءا بالعامل البسيط إلى غاية من هم في أعلى الهرم، لتبني ثقافة حماية المعلومة لا بد أن يكون باستمرار وعلى نطاق واسع بُغية تسهيل التعامل السريع مع المستجدات الطارئة التي قد تفاجئ المؤسسة من حين لآخر، والبحث عن آليات وإجراءات جديدة تحقق التنبؤ بالتهديدات وبالتالي التفتن لها.

كلمات مفتاحية: الاختراق، الجرائم المعلوماتية، الخصوصية، الأمن المعلوماتي.

Abstract

We aim through this intervention to know the digital world's impact on the stability of the information security in the economic institution and to show the extent of guarantee and protection of the individual's privacy in particular and institutions in general.

Considering the importance of technology in our time, its exploitation has become inevitable for both individuals and institutions. The digital revolution in the field of communication and information has led to many new variables of information security in its digital form, the relationship with the internet has become evolving and it gets complicated little by little and individual's life and the institutions business are all connected to the internet! Everything has become intertwined and complicated.

And here preserving the privacy of the institutions has become really important, and hard to control in the same time, and the situation worsens with the spread of hackers of other's privacy, especially with the intensification of competition between the economic institutions, so they need to be careful by following the security procedures.

Renewing the thinking of all employees in the institution starting with the simple employee to those who are on the top of the pyramid, to adopt a culture of information protection, it must be continuous and on a large scale, and this is what facilitates the quick dealing with the emergencies which may surprise the institution from time to time, and searching new procedures that achieve prediction of threats and therefore to be aware of them.

Keywords: information security, privacy, hack, information crimes.



رقمنة مجلة الدراسات الإعلامية والاتصالية

المجلد 03 | العدد 01 (خاص)

مارس 2023

الصفحات 31 - 43

ردمك | ISSN-2773-4285

EISSN | 2830-8417

الإيداع القانوني | 03/2023

العنوان | 11، طريق دودو مختار، بن عكنون، الجزائر العاصمة.

الفاكس | 23 88 50 (023)

الهاتف | 62 29 75 (0561)

تاريخ الاستلام 2022/12/06

تاريخ القبول 2022/12/15

تاريخ النشر 2023/13/18

د. إيمان بن نعجة |

الاسم الكامل

جامعة الجزائر 3 (الجزائر)

imenebennadja@univ-alger3.dz



1. مقدمة:

أصبح أمن المعلومات من الاهتمامات الكبرى للأشخاص والمؤسسات سواء العامة أو الخاصة لوضع حواجز أمنية وأخذ تدابير لمكافحة السلوكيات غير المشروعة أو التهديدات الضارة والمرتكبة ضد المعلومة سواء بصورة مباشرة أو عبر التكنولوجيا لحماية المعطيات الشخصية، وتقوية أمن المعلومات الاستراتيجية في المؤسسة.

فاختراق المعلومات يشكل خطرا يسبب خسائر للاقتصاد وللمؤسسات التي تمثل البنية التحتية الحيوية للدول، وأمن المعلومة يعد أولوية استراتيجية أساسية لتطور المؤسسات.

لذلك سنطرح أهم عناصر الأمن المعلوماتي في المؤسسات الاقتصادية، وتبنى سياسة أمن المعلومات على أساس حاجة المؤسسة والمخاطر التي تتعرض لها، ومن الواجب فهمها والالتزام بتطبيقها، فأمن المعلومات يتطلب إجراءات فنية وإدارية مما يستدعي وعي كل الأطراف العاملة في المؤسسة بالمخاطر التي تهدد المعلومة والسهر على تطبيق الإجراءات والمعايير الأمنية وتحمل نتيجة عدم الالتزام بذلك من خسائر مادية ومعنوية.

2. المخاطر الرقمية والمفاهيم المرتبطة بها

1.2 مفهوم الجريمة المعلوماتية:

تضم الجريمة المعلوماتية جملة من المصطلحات التي لا بد من التفرقة بينها من خلال تحديد تعريف كل واحد منها وهي كالتالي:

تعريف الاعتداء الإلكتروني: والذي يهدف إلى إلحاق الضرر بالجهاز الذي يصيبه، وذلك بالتأثير على سلامة المعلومات وسريتها أو توافرها عند الحاجة إليها وهو يأتي من مصدر إلكتروني قد يكون وسائط التخزين المختلفة وشبكات الاتصال الداخلية والخارجية للمؤسسة (Intranet et Extranet) أو من شبكة الانترنت (Internet).

تعريف التهديد: يعني الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصا، أو شيئا يهدد الأجهزة أو البرامج أو البيانات، أو حدثا كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية.

تعريف نقاط الضعف أو الثغرات: تعني عنصر أو نقطة أو موقع في النظام يحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق وهي الأسباب المحركة لتحقيق التهديدات أو المخاطر.

تعريف المخاطر: تقوم استراتيجية أمن المعلومات الناجحة على تحليل المخاطر، وتعني التساؤل حول التهديدات ثم نقاط الضعف وأخيرا وسائل الوقاية المناسبة للتعامل مع التهديدات ووسائل منع نقاط الضعف.

تعريف الحوادث: ويشير إلى الأفعال المقصودة أو غير المقصودة، والتي قد تكون مخاطر بفعل الطبيعة ودون عامل قصدي، ويغطي الاعتداءات والأخطاء الفنية كذلك.

تعريف الهجمات: هو اصطلاح يستخدم كمرادف للاختراقات والاعتداءات، بحيث توصف به مختلف أنماط الاعتداءات التقنية. (حديد، كريبط، 2014، ص188)

2.2 المؤسسات الاقتصادية في زمن الجريمة الإلكترونية

تغيرت أنماط الجريمة، ولم تعد الاعتداءات تستهدف النفس والمال فقط، بل طالت المعلومات، وهو ما أصبح يعرف على الساحة الدولية بإجرام ذوي الياقات البيضاء، حيث يستطيع المجرمون العصريون ارتكاب أبشع الجرائم، ليس فقط دون إراقة دماء، ولكن أيضا بدون الانتقال من أماكنهم، فهذا النوع من الجرائم ليس مقصورا على منطقة، أو دولة معينة، لكنها مشكلة عالمية (عطوي، 2012، ص 8).

وبتغير أنماط الجريمة فقد تعددت الجهات التي تخترق أمنية المعلومات أيضا إلى الحد الذي قد يتعذر معه أحيانا الكشف عن الجهة الحقيقية التي تقف وراء هذا الاختراق، فالذين لم يعتادوا على حجم المشكلات الملازمة لأمن المعلومات قد لا يمتلكون فكرة واضحة عن تلك الجهات التي تخترق أمن المعلومات. (داود، 2000، ص 515).

3. أنواع الاعتداءات الالكترونية:

نظرا لكثرة أنواع الاعتداءات الالكترونية التي تواجهها المؤسسات، سنذكر أهمها وهي:

أ. استعمال البرامج الخبيثة:

هناك العديد من البرامج الخبيثة، والتي تستعمل للاعتداء الإلكتروني على المؤسسات، ومن مجملها:

- الفيروسات: وهي عبارة عن برنامج صغير ينسخ نفسه على أجهزة الحاسب، وله قدرة تخريرية كبيرة تتراوح من إلغاء البيانات أو إلغاء جدول توزيع الملفات إلى عمل خدوش في القرص الصلب نفسه،
- حصان طراودة: هو برنامج فساد مخفي في برنامج آخر صحيح ويقوم بعمليات فساد تتمثل في إعطاء دخول للحاسوب الذي تشتغل عليه بفتح باب خلفي،
- الهوكس: وهو ترويج لبعض المعلومات الخاطئة عن طريق البريد الإلكتروني من ظرف بعض الجهات، حيث تحرض الرسالة المستقبلية الشخص المستقبل بتحويلها وإرسالها بدوره إلى أشخاص من محيطه، والهدف من هذه العملية هو انسداد الشبكات بسبب التسرب الكبير للمعلومات في نفس الوقت.
- الدودة: هي نوع من أنواع الفيروسات الذي تنتشر عن طريق الشبكة، والتي بدون الفيروسات لا يمكنها التكاثر في الشبكة، هذا البرنامج الخبيث يمكن أن يكون على شكل BOT، يتم التحكم فيه عن بعد.

ب. استعمال برامج الجوسسة:

برامج الجوسسة تستغل في الاستخدام غير المشروع للمعلومات، من خلال تثبيتها بداخل النظام، حيث تتواصل مع وكيل خارجي عن طريق ما يعرف بالباب الخلفي (Bloch; Wolfhugel , 2008, 60).

لهذا فإن حماية المعلومة تعدّ اهتمام جميع الفاعلين المعنيين في المؤسسة، ومن الضروري أن يكون كل منهم على وعي بمدى حساسية وضعف المعلومات التي يمتلكها، والممارسات الاحتياطية القائمة والحاجة إلى نشر السيطرة والتحكم في هذه المعلومات داخليا وخارجيا، كما يجب على سياسة إدارة البيانات أن تساهم في الحفاظ على سلامتها وتوافرها، وسريتها أيضا، كما يجب أن تسمح الإجراءات الواجب اتباعها بالعمل بكل ثقة مع المتعاونين معها، وأن تكون أفضل تسلحا لتصدي جميع الطرق غير الشرعية (قرصنة المعلومات، التجسس الاقتصادي، التزوير ...) (Wauquiez , 2012, 19).

ولم تقتصر لهذا الحد فقط بل أصبحت الهجمات الإلكترونية أداة قوية لشن حرب إلكترونية حكومية من قبل الأفراد المستقلين، أو وسيلة حرب إلكترونية اقتصادية بين مؤسسات متنافسة، وأصبح الهدف من عمليات الاختراق ليس الحصول على المال فقط من خلال اختراق مؤسسات الأموال وابتزازهم وتهديدتهم، بل تعدت المال لتصبح وسيلة لإعلان مواقف سياسية أو الانتقام أو المقاومة، وهذا ما سنتناوله في العنصر الموالي.

4. قرصنة المؤسسات واختراق حدود الحكومات والخسائر الناجمة عن ذلك:

1.4 على المستوى العالمي:

يُحتمل افتعال الهجمات الإلكترونية بين الحكومات ضد بعضها البعض في إطار ما اصطلح على تسميته بالحروب الإلكترونية، مثلما قامت به أمريكا عام 2010 حيث أرسلت فيروس Stuxnet بُغية تخريب البرامج النووية الإيرانية التي يُشتبه في اعتمادها لصناعة السلاح النووي (noonpost, 2015).

وخلال عام 2011 عرف العالم جماعات متخصصة من القراصنة الإلكترونيين، مثل Anonymous و LulzSec وغيرهما، حيث استهدفت تلك الجماعات الشركات والأفراد لتحقيق مآرب سياسية مختلفة. ويرجع خبراء شركة تريند مايكرو -إحدى الشركات الدولية المتخصصة في أمن المعلومات- أن تزداد أنشطة مثل هذه الجماعات خلال عام 2012، بل وأن تزداد قدرتها على اختراق شبكات الشركات والإفلات من محاولات رصدها ومقاضاتها (غيطاس، 2012).

إن "الفاتورة" الإجمالية لجرائم أمن المعلومات عالمياً وعربياً في 2011 وحده تقدر بحوالي 388 مليار دولار أمريكي، أما التكلفة النقدية المباشرة لهذه الجرائم والمتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجمات فتقدر بحوالي 114 مليار دولار.

وقد توزعت هذه الجرائم ما بين جرائم الفيروسات والبريد الإلكتروني الملوث والضار، وجرائم الاحتيال والنصب والاصطياد، والجرائم المتعلقة باختراق الهواتف المحمولة.

وفي 2012 تعطلت مواقع إلكترونية لعدة بنوك أمريكية، فيما اتهم مسؤولون أمريكيون أن إيران قامت بهذا الهجوم للرد على العقوبات الاقتصادية على برنامج إيران النووي، وكان الهجوم مكلفاً ملايين الدولارات للبنوك الأمريكية.

● اختراق شركة SONY

الاختراق الذي كلف شركة SONY عشرات الملايين من الدولارات قام به مجموعة من المخترقين أطلقوا على أنفسهم مسعى "فرسان السلام"، ويُعتقد أنهم قراصنة من كوريا الشمالية قاموا بالاختراق لإجبار الشركة على إيقاف عرض فيلم The Interview الذي يستهزئ برئيس كوريا الشمالية، وحجم الأضرار التي تسبب بها هذا الاختراق كان كبيراً جداً، حيث تم سرقة 77 مليون إيميل و12700 بطاقة ائتمان واختراق 25 مليون حساب لمستخدمي SONY، كما تم تسريب أفلام لم تعرض بعد وسيناريوهات لأفلام ستصور قريباً، ويُتوقع أن تبلغ قيمة الخسائر 100 مليون دولار وانخفضت أسهم بورصة سوني 6.6%.

وبعد تنفيذ الاختراق واتهام كوريا الشمالية انقطع الاتصال بالإنترنت في أنحاء كوريا الشمالية لأكثر من 9 ساعات، ثم انقطع مرة أخرى في اليوم الذي يليه، واتهمت كوريا الشمالية الولايات المتحدة الأمريكية بهذا ولم يعلق الرئيس أوباما على ما حدث (noonpost, 2015).

• اختراق شركة "Solarwinds"

في عام 2020 أشارت أغلب التقارير الصحفية إلى اختراق ثغرة أمنية داخل برنامج توفره شركة "Solarwinds" لمراقبة البرمجيات، وهي شركة يقع مركزها الرئيسي في مدينة أوستن بولاية Texas، ومن أهم البرامج التي توفرها الشركة لجهات حكومية مهمة برنامج "Orion" لمراقبة وتأمين شبكات الحاسوب الخاصة بها، والذي تم الاختراق عن طريقه، وهذا الاختراق يأتي ضمن قائمة طويلة من الهجمات الإلكترونية التي يشتبه بأن روسيا قامت بشنها (Reuters)، معتقدين أن سبب الاقتحام يمكن أن يكون ببساطة حالة تجسس من حكومة تحاول فهم ما يفعله خصمها (المنشاوي، 2020).

2.4 على المستوى العربي والوطني:

لا يقف خطر القرصنة الإلكترونية عند الدول الكبرى فقط، ففي العالم العربي تصل خسائر القرصنة سنوياً إلى عشرة ملايين دولار، وتعرف الدول العربية انتشاراً كبيراً للبرمجيات الخبيثة بنسبة تجاوز عشرة أضعاف المعدل العالمي، وذلك في ظل غياب مهول للأمن المعلوماتي. وحسب تصنيف الدول الخاص بالسلامة والأمن المعلوماتي الذي تنجزه مجموعة مايكروسوفت العالمية، فإن العراق والمغرب والأردن يتصدرون الدول الأكثر تعرضاً لهجمات القرصنة والبرامج الضارة على نظمته المعلوماتية، ويرجع ذلك إلى استفحال ظاهرة القرصنة في العالم العربي، مما يضعف الجدارية الإلكترونية للمؤسسات ويفتح الباب على مصراعيه أمام التجسس المعلوماتي (بلفلاح، 2015).

وقد أكد الخبير الدولي في الأمن المعلوماتي عبد العزيز دردوري، أن الشبكة الجزائرية غير مؤمنة، بالنظر إلى عديد الأسباب أبرزها غياب رؤية إستراتيجية مستقبلية لبناء جدار قوي لحماية المواقع الوطنية، وسياسة "اللامبالاة" وعدم الاكتراث بالمخاطر التي يمكنها هدم منظومة دولة بأكملها، سيما في الجانب المتعلق بالأمن والدفاع الوطني، وكذا غياب مؤسسات جزائرية متخصصة في الأمن المعلوماتي.

فأي اختراق تكون نتائجه مكلفة، من حيث مدة اكتشاف أثار التخريب، وإصلاح الأعطاب والتي تكلف خسائر مالية وكذا تحويل واستغلال قواعد البيانات، لنحو مليون زبون، لهذا فإن التجسس الاقتصادي والصناعي من أخطر أهداف الاختراق المعلوماتي.

أما رئيس الجمعية الجزائرية لمؤني خدمات الانترنت، علي كحلان، فيقول إن النظام المعلوماتي في الجزائر مهدد بالاختراق، أمام عجز الحكومة على حماية قاعدة بيانات الجزائريين بما فيها مؤسساتها الرسمية، وأبرز المتحدث خطورة استعمال برامج استغلال مقرصنة وكذا برامج الحماية من الفيروسات، مؤكداً أن المؤسسات الاقتصادية معرضة أكثر من غيرها للاختراق والتجسس، لهشاشتها أو غياب برامج الحماية، داعياً إلى إنشاء مؤسسة متخصصة في تسيير النظام المعلوماتي في الجزائر على شاكلة الدول المتطورة، معتبراً حماية الأمن المعلوماتي قضية دولة (الشروق أون لاين، 2011).

كما أشارت الإحصائيات إلى تسجيل 3500 اختراق لمواقع جزائرية من الخارج، منها 990 اختراق لمواقع إخبارية في ظرف سنة واحدة دون تسجيل أي شكوى رسمية واحدة لدى مصالح الأمن .

كما شكلت حالة الجزائري بن دلاج الذي تم توقيفه في بانكوك من طرف الشرطة الفدرالية الأمريكية "أف.بي.أي" نموذجا حول طريقة الاختراق وتحول الأموال، وانتقد مختصون بالمناسبة ضعف التنسيق مع الخارج في مجال مكافحة الجريمة الإلكترونية باستثناء حالة واحدة تم تسجيلها، وتخص التنسيق الذي حصل بين الجزائر وال "أف.بي.أي" فيما يتعلق بقضية أحد المطلوبين في جريمة إلكترونية (عبد السلام، 2013).

وكانت أكبر قضية تكشف هشاشة أنظمة الحماية الخاصة بالبرامج الآلية لأحد أكبر المؤسسات الاقتصادية بالجزائر «ألجيري تيليكوم»، حيث فضحها «الهacker» الشاب الذي أقر بوجود ثغرات كبيرة في أنظمة الحماية التقنية للبرامج الآلية في الشركة، مما يجعلها عرضة للقرصنة كون أغلبها قديمة ولم تجدد منذ عهد.

وتعرض النظام المعلوماتي للشركة لعدة اختراقات، بين شهر جوان إلى نوفمبر 2017، بعد اختراق البريد الإلكتروني لأحدى الموظفات والعبث به، حيث تم من خلاله إرسال رسالة إلكترونية إلى كافة المسؤولين يحمل ملفا إلكترونيا لبرنامج للتحميل pdf، تبين بعدها أنه فيروس يقوم بعد النقر عليه بالتموقع على النظام الآلي لجهاز الحاسوب، مما يسمح للمخترق بالتجسس على قاعدة المعطيات والتحكم فيها.

وهو ما مكن «الهacker» من التهديد بتحميل جميع المعطيات وملفات الفوترة الخاصة بزبائن ومتعاملي مؤسسة «اتصالات الجزائر»، بما فيها من إدارات ووزارات وهيئات رسمية. ليتم اكتشاف ولوج نفس «الهacker» إلى النظام عدة مرات خارج أوقات العمل، وتم اكتشاف إضافته لبرامج ضارة موجهة لأنظمة الحماية الخاصة بالبرامج والدخول إلى شبكة الأنترنت الحالية، وتغيير وتعديل في الشبكة والدخول إلى الذاكرة المركزية للمؤسسة، وعليه تم تقديم شكوى ثانية خاصة بعد تلقي مدير المنشآت التحتية للنظام الآلي رسالتين تهديد، اعترف فيها المتهم بامتلاكه الأرقام السرية للأنظمة المعلوماتية، وقام المخترق بتطوير الفيروس، مما مكنه من تعطيل الشبكة على المستوى الوطني، وبعد تحقيقات قام بها التقنيون بالمؤسسة تم التوصل بالتنسيق مع فرقة مكافحة الجريمة الإلكترونية إلى تحديد هوية الهacker (ق. جميلة، 2017).

من جهة أخرى توصلت الباحثة بن اعراب أمال في نتائج دراستها الاستطلاعية على 110 مؤسسة اقتصادية جزائرية حول حماية المعلومات وسلوكيات المؤسسة الجزائرية، بحيث أن معظم أصحاب المؤسسات يقومون بإسناد مهمة حماية معلومات المؤسسة لإدارة أمن المعلومات بالدرجة الأولى، كما أن أغليتهم يتبنون السياسة الأمنية للمعلومة لكلا المحيطين الداخلي والخارجي، بحيث هذين المحيطين كلاهما مصدر خطر وتهديد للمؤسسة لا بد من أخذ الحيطة منهما خاصة فيما يتعلق بالفاعلين الموجودين في المحيط الخارجي، إلا أن هذا الأخير أخذ النصيب الأكبر من تسخير متطلبات الحماية والأمن، نظرا لعدم ارتياح المسؤولين لهذا المحيط بما فيه من منافسين وأعداء للمؤسسة،

وبذلك تصدر البيئة الخارجية حالة اللا-إرتياح لدى أصحاب المؤسسات، نظرا للمنافسة الشرعية واللاشرعية، وغياب بعض القوانين والتشريعات التي تحمي المؤسسات تزيد من الخوف لدى أصحاب المؤسسات، وبالمقابل يشكّل كل من العنصر البشري والعنصر التكنولوجي مصدرا تهديد لمعلومات المؤسسة، إلا أن معظمهم يرون أن العنصر البشري الخارجي (المنافسين

وأعداء المؤسسة)، يشكل تهديدا لمؤسساتهم بالدرجة الأولى، والعنصر البشري بصفة عامة بغض النظر عن البيئة المتواجده فيها (داخلية كانت أم خارجية) هو الأكثر تهديدا من العنصر التكنولوجي، وهذا ما أكدته الدراسة، بحيث أن وراء أي تهديد أيا كان نوعه نجد أن مسببه هو العنصر البشري بقصد أو بغير قصد وبغض النظر عن الوسيلة المستخدمة في ذلك.

بصفة عامة يمكن القول أن هناك نسبة لا بأس بها من المؤسسات تعاني من المخاطر التي تندرج تحت سقف سوء استخدام المعلومات، وعلى رأسها التجسس الصناعي (التنافسي)، ثم يليها خطر الإهمال، وتتصدرها اتخاذ قرارات غير صحيحة عند التعامل مع معلومات المؤسسة، ثم تليها خطر تدمير المعلومات من خلال استخدام الفيروسات، مثل التعرض لتهديد حذف الملفات وإعادة تسميتها وتغيير توزيع الملفات المخزونة، أما فيما يخص مجموعة التجسس التنافسي (الصناعي) باعتبارها مصدر رابع مهدد لمعلومات المؤسسة، نجد أن الاطلاع على المعلومات الظاهرة على شاشة الحاسب هو المهدد الأول الذي تعاني منه بعض المؤسسات المبحوثة، ثم يأتي خطر سرقة المعلومات وتسريبها، بحيث أن أغلبية المؤسسات لا تعاني من معظم التهديدات التي تندرج تحت مضلة هذا الخطر، إلا أن هناك نسبة قليلة من تعاني من التسلل البدني لأماكن العمل واختلاس اجراءات العمل.

وعلى العموم يمكن القول أن محيطنا الاقتصادي ليس في معزل عن هذه الجرائم المعلوماتية، فهناك بعض الحالات الخطرة لبعض المؤسسات التي تعاني من بعض المخاطر باختلاف طبيعتها، وهذا ما يدعو لأخذ الحيطة والحذر من هذه الظاهرة التي إذا ما تم إيجاد العلاج المناسب لها في بداية انتشارها فإنها ستستمر في التوغل نحو مؤسساتنا لتهديد اقتصادنا الوطني (بن أعراب، 2021، ص 319).

5. الأمن المعلوماتي بين المفهوم والمسؤولية والإجراءات الحمائية:

1.5 مفهوم الأمن المعلوماتي:

يمكن تعريف أمن المعلومات من خلال ثلاثة زوايا:

يُعرف أكاديميا بأنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها.

أما قانونيا فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات (بوفاس وطلحي، 2014، ص 3).

كما يُعرف تكنولوجيا بأنه "حماية أصول وموارد ومكتسبات نظام معلوماتي ما بطرق مشروعة، وهو أيضا أداة تتحكم في تنظيم العلاقات والاتصالات، وذلك دون أن يؤثر على قدرة مستخدمي هذا النظام على الأداء أو يعوق عملهم من حيث الكفاءة أو التوقيت" (الدسوقي، 2009، ص 515).

وعليه، يتطلب على المؤسسة حماية كل ما له علاقة بالموارد المعلوماتية، وحتى تؤمن المؤسسة نفسها لابد من تأمين مواردها البشرية والموارد التكنولوجية من الحواسيب المستخدمة و وسائط المعلومات التي تحتوي على بياناتها وخصوصياتها الهامة، وذلك في جميع مراحل تواجد المعلومة (التخزين- النقل- المعالجة).

2.5 مسؤولية الأمن المعلوماتي في المؤسسة:

تعدّ الادارة العليا المسؤولة عن توفير الأمن والحماية للمنشأة، وهذه المسؤوليات تندرج من مستوى إداري إلى آخر (بوفاس وطلحي، 2014، ص 4):

- أ. مسؤولية قمة الهرم الإداري: هي وضع الإطار العام لسياسات أمن المؤسسة والإقرار بالمسؤولية عن حمايتها.
- ب. مسؤولية إدارة أمن نظم المعلومات: تقع مسؤولية وضع السياسات الأمنية وتطبيقها على عاتق إدارة متخصصة مناط بها تطبيق رغبة الإدارة العليا في حماية المؤسسة وأصولها.
- ج. مسؤولية مالك البيانات والمعلومات: تؤول ملكية المعلومات ونظم المعلومات وأصولها إلى جهات أو أفراد داخل المؤسسة، ويكون المالك هو المسؤول المباشر عن كل ما يتعلق بتأمين المصادر تحت ملكيته مثل تحديد نوع الحماية المطلوبة وتحديد الصلاحيات الممنوحة للمستخدمين...الخ.
- د. مسؤولية خدمة البيانات والمعلومات: وتتم عادة من موظفي التقنية والمسؤولية تقع على إدارة النظم وصيانة المعلومات وتحديثها وعمل النسخ الوقائي.
- هـ. مسؤولية المستخدمين: هم الأشخاص الذين يقومون باستخدام البيانات بشكل روتيني من خلال الصلاحيات الممنوحة لهم لأداء العمل بصورة لا تشكل تهديدا لأمن نظم ومعلومات المؤسسة، وتقع حدود مسؤوليتهم في الاستخدام الشرعي للنظام في حدود صلاحياتهم.

3.5 أهم الإجراءات الأمنية لحماية خصوصية للمؤسسات:

إن "تحقيق الأمن والخصوصية لا يتناقض، بل هما أمران متلازمان، حيث لا يمكن للفرد أن ينعم بالخصوصية إلا إذا شعر بالأمان، كما أنه لا يمكن أن يحس بالأمان إذا لم يتمكن من ممارسة خصوصيته" (أبو نعمه، 2017).

والوعي بحماية المعلومات شديد الأهمية لأي استراتيجية أمن خاصة بالمؤسسات ودعم عمليات الأمن المعلوماتي، وعلى الرغم من أهمية توعية المستخدمين بدورهم ومسؤوليتهم في الأمن المعلوماتي فإن 64% من المنظمات في أمريكا، و 48% من منظمات إنجلترا، 59% من منظمات الهند فقط تقوم بتوفير برامج توعية أمنية على الرغم من اللوائح التي تأمر بذلك، والكثير من الحوادث التي تؤدي إلى خسارة ملايين الدولارات كغرامات وخسارة السمعة التي كان من الممكن تجنبها بتوفير وعي وتدريب مناسب للمستخدمين والتقنيين والمديرين (العلي وآخرون، 2006، ص 215).

فجميع المؤسسات لديها معلومات مهمة يجب حمايتها بطريقة أو بأخرى، وفي حالة فقدان هذه المعلومات أو الكشف عنها، يمكن أن تكون العواقب وخيمة بالنسبة للمؤسسات، خاصةً من حيث صورة المؤسسة، انخفاض حجم المبيعات أو خسارة في حصة السوق.

ويمكن للتكنولوجيات (الموجهات والجدران النارية والتشفير) حل بعض المشاكل المتعلقة بأمن تكنولوجيا المعلومات، ولكن لا يمكن أن تحل محل قواعد الممارسات الجيدة في هذا المجال، لذلك فمن المستحسن أن تقوم الإدارة بتحليل المخاطر حالة بحالة لتحديد مستوى الضوابط المطلوبة والحصول على معلومات محمية، هذه الضوابط يجب أن تضمن نسخ احتياطية مع ضمان وصول المعلومات لمن يحتاجونها. كما أن ترتيب وظيفة الذكاء الاقتصادي داخل المؤسسة، يساعد بشكل أو بآخر على معالجة المعلومات وتخزينها بطريقة آمنة (Delecroix, pp 98 – 99).

وعلى هذا الأساس يمكن للمؤسسة تدعيم استراتيجيتها الأمنية بإجراءات تعتبر مهمة وهي:

• تحديد الأسرار التجارية

الأسرار التجارية تختلف عن حقوق الملكية الفكرية الأخرى. فعلى عكس حافطة الحقوق المسجلة أو غير المسجلة- مثل قائمة المصنفات المنشورة- حافطة الأسرار التجارية هي، على نحو ما وصف مارك هاليغان وريشار وياند، في مؤلفهما المعنون "Trade Secret Asset Management (2006)" عبارة عن "سحابة غير ملموسة ومتفرقة من المعلومات المخزنة في أوراق، وفي حواسيب وفي عقول الموظفين".

وقد يكون من الصعب تعريف مفهوم السر لكنه ضروري عند مطالبة محكمة بأن تصدر حكماً لوقف متعدي عن إساءة استخدام المعلومات التي يحميها السر. ويحق للمدعى عليه أن يعرف تحديداً ما لا يمكنه استخدامه، وتتوقع المحكمة أن يعرف المدعي ما الذي يدعي أنه يمتلكه وينبغي له حمايته.

• أنظمة تكنولوجيا معلومات محمية

إن تهديد الإنترنت لأنظمة الحاسوب (البرمجيات المؤدية وفيرس الفدية وما إلى ذلك) موثق بشكل جيد. وينبغي أن تضع المنظمات تدابير أمنية (تشفير البيانات، ووضع ضوابط بشأن كلمة السر، والحماية من الفيروسات) وينبغي أن تتماشى الإجراءات المتخذة مع مستوى المخاطر التي يتصور أنها تهدد المعلومات المعنية وقيمتها.

• الضوابط المادية

لدى معظم المنظمات ضوابط على عملية النفاذ. وهنا أيضاً، يتوقف مستوى الإجراءات الأمني المطبق على الزوار وعلى الموظفين، على المخاطر التي تواجه المنظمة. ووفقاً لتقرير إخباري نشر مؤخراً في مجلة الصنداي تلغراف في المملكة المتحدة، تخطط بعض الشركات في المملكة المتحدة "تزويد موظفيها برقاقة صغيرة" (عن طريق إدخال رقاقة حيوية تحت الجلد) لوضع ضوابط أوتوماتيكية على النفاذ ومن ثم حماية المجالات الحساسة للشركة. وتخضع للنقاش مسألة ما إذا كان مثل هذا الإجراء المتطرف يتناسب مع المخاطر التي تواجهها الشركة.

• الأمن الوثائقي

معظم المعلومات السرية تسجل وتنقل داخل المنظمة وخارجها في شكل وثائقي. ويشكل وضع عبارة "سري" على الوثائق المطبوعة أو الإلكترونية إجراءً أساسياً لكنه مهم حيث يتعين على الشركات ألا تغفله. فهو يثبت أن الشركة لفتت الانتباه إلى ضرورة إخفاء المعلومات المعنية.

• سياسة إنفاذ

إن اللجوء إلى إنفاذ حقوق ضد شخص تملك أسراراً تجارية أو كشف عنها بشكل غير مشروع يعني فشل الجهود المعقولة. وهو أمر غير مبرر تماماً. وهناك دوماً خطراً إساءة الاستخدام أو الإفصاح من جانب متعدد محدد أو سوء النية، رغم الجهود التي يبذلها صاحب الحق.

إن وجود سياسة إنفاذ قائمة واستخدامها بنجاح يمثلان أمرين مختلفين، نظراً لأن التقاضي ينطوي على آثار من حيث التكلفة والمخاطر. غير أنه بملاحظة المتعدين، توجه المنظمة رسالة بأنها ستتخذ الإجراءات اللازمة للحفاظ على حقوقها القيمة وحمايتها (WIPO, 2019).

ولضمان خصوصية معلومات المؤسسات ارتأينا تقديم بعض الخطوات التي نراها أساسية لتحقيق الهدف المبتغى من وراء الأمن المعلوماتي، وتتمثل هذه الخطوات فيما يلي:

- فحص البيانات التي تم جمعها وتخزينها والسبب المرتبط بها:

وفي هذه الخطوة من المهم التفكير في المعلومات التي تحتاجها حقاً في خدمة عملاء المؤسسة، وكلما زادت البيانات المجمعة كلما زادت المخاطر التي تتعرض لها وكلما زادت أيضاً تكاليف هذه البيانات، وأصبح البحث عنها أكثر تعقيداً سواء كانت مخزنة في ملفات ورقية أو وسائط رقمية.

والإدارة الجيدة للبيانات تتطلب استراتيجية تجميع وغرلة للمعلومات لابقاء ما يتماشى مع احتياجات المؤسسة وتوقعات العملاء من حيث السرية.

- تحديد من له حق الوصول إلى البيانات:

ولتجنب الوصول غير المصرح به للمعلومات هناك عدة طرق، أهمها تحديد أدوار الأفراد المسموح لهم بالوصول للمعلومات الخاصة بكل فرد، وبعد ذلك يتم منح امتيازات لبعض الأفراد، وتقييد أفراد آخرين، وهذه الطريقة هي الأفضل إلا أن معظم المؤسسات لا تعتمد على هذا المبدأ.

- فهم وإدراك المخاطر المرتبطة بالبيانات:

يجب على المؤسسة مراعاة مخاطر البيانات، بما في ذلك:

- قيمة البيانات،
- التكلفة التي تترتب عن فقدان البيانات،
- النتائج المترتبة عن جمع البيانات ذات خصوصية،
- تكلفة الحلول الممكنة لمواجهة الخطر.

إن تقييم المخاطر يساعد على تحديد مدى الحاجة لإضافة فحوصات أمنية أخرى لتقليل أو تحويل أو تجنب الخطر من خلال تعديل العملية.

- تدريب وتوعية الموظفين بدورهم في خصوصية البيانات :

بعد الخطأ البشري والتصرفات غير المسؤولة من الأسباب الشائعة للانتهاكات الإلكترونية، وللكف من ذلك لابد من تدريب الموظفين وتحسيسهم بأهمية الأمن الإلكتروني والحفاظ على خصوصية البيانات ودورهم الفعال في المساهمة في تحقيق ذلك.

هذا التدريب يساعدهم على فهم المخاطر الناجمة عن عدم التقيد بروتوكولات سرية وخصوصية البيانات التي تنعكس سلباً على المؤسسة وعملائها، وفي هذا الصدد نجد الموظفون الأكثر معرفة بهذا الشأن قادرون على اكتشاف وتجنب الجرائم الإلكترونية المنتشرة وتهديدات الخصوصية، وهذا يعود بالفائدة على المؤسسة. (Mohmud . 2022. BDC)

6. خاتمة:

إن تحقيق تقدم ملموس في قضية أمن المعلومات عالمياً أو عربياً لن يتم إلا بتغيير المنهج القائم حالياً والذي يتعامل مع القضية باعتبارها قضية "تقنية بحتة" تقع مسؤوليتها على الفنيين والمختصين في علوم الحاسب وتأمين الشبكات، إلا أن التهديدات والأخطار التي تستهدف المعلومات تختلف، ومعظمها نجدها في المجال الاقتصادي لتحقيق مكاسب اقتصادية وكثيراً ما تتعدى ذلك لتصبح ذات أهداف سياسية بين الحكومات، فالحرب الاقتصادية لا تقل في شدتها حالياً عن الحرب العسكرية، فباعتبار المؤسسات الاقتصادية التي تمثل البنية التحتية لأي دولة فإن الأمر يتطلب أمن وحماية المعلومات والذي يتجسد من خلال الإجراءات التي تتخذ للحفاظ على سلامة المعلومات من التخريب العبث والفقدان والكشف.

كما نؤكد على ضرورة وجود إطار استراتيجي عملي وشامل لأمن معلومات يتصف بهيكله وصياغة جيدة وسهلة الفهم من قبل جميع مستويات أعضاء المؤسسة والتحسيس بأهمية المعلومة وزيادة وعيهم بتوفير الحماية اللازمة لها، ومواكبة كافة المتغيرات الخاصة بالمعايير العالمية وتبنيها في إطار التطور والحدثة والتحسين المستمر.

7. قائمة المراجع:

1. الشريف بوفاس، فاطمة الزهراء طلحي: نحو بناء نظم لإدارة حماية المعلومات ISO27001 في المؤسسات الجزائرية. المؤتمر الدولي الثاني للذكاء الاقتصادي حول "اليقظة الاستراتيجية ونظم المعلومات في المؤسسة الاقتصادية"، أيام 29/30 أبريل 2014 جامعة باجي مختار/عناينة، ص 3.
2. طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.
3. مليكة عطوي، الجريمة المعلوماتية، حويلات جامعة الجزائر، العدد 21/جوان 2012.
4. حسن طاهر داود، جرائم نظام المعلومات، مكتبة الملك الفهد الوطنية للنشر، أكاديمية نايف للعلوم الأمنية، الرياض، ط1، 2000.

5. اختراق المؤسسات والشبكات: وسيلة مقاومة وأداة للردع <https://www.noonpost.com/content/5619> تم الاطلاع على الموقع يوم 20-11-2022 على الساعة: 14:20.
6. جمال محمد غيطاس، كل ما تريد معرفته عن عملية الاختراق الكبرى للمؤسسات الأميركية <https://studies.aljazeera.net/ar/issues/2012/02/2012229132228652960.html> تم الاطلاع على الموقع يوم 13-11-2022 على الساعة 14:40.
7. محمد المنشاوي 16/12/2020، تم الاطلاع على الموقع يوم 24-11-2022 على الساعة 14:30 [من-اكثر-العمليات-ضرا-خلال-السنوات](https://www.aljazeera.net/news/scienceandtechnology/2020/12/16/من-اكثر-العمليات-ضرا-خلال-السنوات)
08. يونس بلفلاح، مخاطر القرصنة على الشركات، 20 يناير 2015، تم الاطلاع على الموقع بتاريخ 25-11-2022 <https://www.alaraby.co.uk/مخاطر-القرصنة-على-الشركات>
09. نوفيل حديد، كربيط حنان، أمن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة، مجلة المؤسسة، العدد 3، 2014.
10. الشروق أون لاين، خبراء في الأمن المعلوماتي يرفعون الراية الحمراء ويحذرون: المنظومة المعلوماتية للجزائر غير آمنة وتعتبر هدفا سهلا للقراصنة، 10/11/2011. <https://www.echoroukonline.com/المنظومة-المعلوماتية-للجزائر-غير-آمن>
11. عبد السلام، 3500 اختراق لمواقع جزائرية والهاكرز شبح المؤسسات، 4 جوان 2013 <https://www.ennaharonline.com/3500-اختراق-لمواقع-جزائرية-والهاكرز-شبح-ا/> تم الاطلاع على الموقع يوم 24-11-2022 على الساعة 15:00
12. ق. جميلة، "قمت بقرصنة أنظمة اتصالات الجزائر للتنبيه على وجود ثغرات خطيرة"، 6 ديسمبر 2017 <https://www.ennaharonline.com/قمت-بقرصنة-أنظمة-اتصالات-الجزائر-للت/>
15. بن اعراب أمال، حماية المعلومات وسلوكيات المؤسسة الجزائرية (دراسة استطلاعية لعينة من المؤسسات الاقتصادية الجزائرية)، أطروحة لنيل شهادة دكتوراه العلوم الثالث في علوم الاعلام والاتصال، كلية علوم الاعلام والاتصال، جامعة الجزائر 3، ص 319، ص 322 (بتصرف، لمعرفة التفاصيل اطلع على الأطروحة). 2021
13. هنادي أبونعمة، أكد ضرورة الرقابة الحكومية على المعلومات، شناير: اختراق الخصوصية شرط لتحقيق الأمن <https://www.emaratalyoum.com/local-section/other/2017-02-13-1.969766> تم الاطلاع على الموقع يوم 15-11-2022 .
14. عبد الستار العلي وآخرون، المدخل إلى إدارة المعرفة، دار المسيرة، عمان، 2006.
15. المنظمة العالمية للملكية الفكرية، حماية الأسرار التجارية: كيف يمكن للمنظمات التصدي لتحدي اتخاذ "إجراءات معقولة"، أكتوبر 2019. https://www.wipo.int/wipo_magazine/ar/2019/05/article_0006.html

تم الاطلاع على الموقع يوم 26-11-2022 على الساعة

16. Bloch L ; Wolfhugel C ; Sécurité infomatique ; Eyrolles ; Paris ; 2008 ; p60.

17. Laurent Wauquiez ; **GUIDE DE L'intelligence Economique Pour La Recherche**; République Française ;

18. Délégation Interministérielle à L'intelligence Economique, 2012.

19. Rowda Mohmud; étapes pour améliorer la confidentialité des données dans votre entreprise
Conseillère d'affaires principale, BDC Services-conseils ; 2022.

تم الاطلاع على الموقع بتاريخ 2022-11-30 على الساعة 14:30 <https://www.bdc.ca/fr/articles-outils/blogue/5-etapes-ameliorer-confidentialite-donnees-entreprise>