الحكومة الالكترونية في عصر الاختراق السيبراني "مفهوم جديد للسيادة"

E-government in the era of cyber hackers
The New Concept of Sovereignty

مالكي إبتسام* جامعة البليدة2 - الجزائر-
Malki ibtissem University of Blida 2 - Algeria -
Malkiibtissem2017@gmail.com

تاريخ الاستلام: 2023/07/10 تاريخ القبول للنشر: 2023/09/21 تاريخ النشر: 2023/10/01

ملخص:

تشكل الحكومات الالكترونية تجسيدا للتطورات التي فرضتها العولمة، بالإضافة إلى التقدم التكنولوجي في عالم الاتصال والمعلومات، حيث أصبحت الدول مُلزمة بمواكبة هذا التطور لتضمن تقدمها ونموها، ولتحقق مكانة دولية مرموقة، إلاّ أنّه بعد نهاية الحرب الباردة تغيرت العديد من المفاهيم في حقل العلوم السياسية والعلاقات الدولية، من بينها مفهومي الأمن والتهديد، ولأن التهديدات التي تواجه الدول لم تعد ذات طابع عسكري فقط، أصبح هذا النوع المتطور من الحكومات يواجه تحديات أمنية خطيرة، أهمّها الاختراق السيبراني.

تهدف هذه الدراسة إلى تحديد أهم المفاهيم الحديثة، لكل من الحكومة الالكترونية والاختراق السيبراني، مع التطرق إلى خطورة عمليات الاختراق على الحكومات الالكترونية من خلال مواجهة أعداء خفية ومجهولة المصدر، مع دراسة كيف ينعكس ذلك على مفهوم سيادة الدول.

الكلمات المفتاحية: الحكومة الالكترونية؛ الاختراق السيبراني؛ التهديد؛ الأمن؛ السيادة.

Abstract:

E-Government represents the confluence of developments driven by globalization and the advancements in communication and information technology. Countries have become obliged to align themselves with these developments-to ensure their progress and growth, and prominent international standing. However, after the end of the Cold War, significant shifts occurred in the realms of political science and international relations, particularly in the conceptualization of security and threats. Threats facing nations has evolved beyond the conventional military domain. These advanced types of governments have started to face serious security challenges; the most dangerous among them is cyber penetration.

This study aims to identify the most important modern concepts associated with both electronic government and cyber penetration, while addressing the danger of penetration operations on electronic governments through confronting the inherent risks of unknown origin, examines how this is reflected in the concept of state sovereignty.
***Key words**: E-government; Cyber penetration; Threats; Safety; Sovereignty.*

مقدّمة:

يقود التطور التكنولوجي وانتشار الانترنت، دول العالم الى الانتقال من نموذج الحكومة التقليدية التي تركّز على رفع الكفاءة الداخلية للمؤسسة، الى نموذج الحكومة الالكترونية التي تضع خدمة المواطن في أولوياتها التي تسعى الى تحقيقها، وعلى هذا الأساس تمّ ضخ قدر كبير من المعلومات التي من شأنها مساعدة المواطنين وتسهيل تعاملاتهم مع الحكومة.

إلّا أنّه لم يعد الأمر مقتصرًا على علاقة الحكومة بمواطنيها فقط، من أجل تلبية احتياجاتهم، بل اتسع هذا النمط لينظم العلاقات أيضا بين المؤسسات مع بعضها البعض وبين المؤسسات والحكومة، وذلك لمزيد من الشفافية وتعزيز الحكم الراشد، فأصبح الاعتماد على المنظومة الالكترونية، في جل مؤسساتها المالية منها وحتى العسكرية لحفظ المعلومات المهمة والحساسة والتي تُعنى بالأمن القومي للدولة، والسبب في ذلك هو تسهيل تبادل هذه المعلومات واتاحتها بشكل منظم بين المؤسسات الحكومية للدولة.

لكن الاشكال الذي نحاول اليوم التطرق اليه، هو ظاهرة الاختراق الالكتروني كتهديد عابر للقارات لهذه الحكومات الالكترونية، وما ينعكس جرّاء ذلك على الأمن المعلوماتي لدول العالم كافة، وبما أنّ هذا التهديد سريع التأثير وكارثي النتائج، صُنِّفت حروبه ضمن حروب الجيل الرابع والجيل الخامس التي لا تستوجب فضاء مادي كساحة معركة تقليدية لتنفيذ الهجوم، ولا تحتاج لأسلحة وجيوش لإحداث خسائر ضخمة للدول المستهدفة، يكفي فقط أن تتوفر للمخترقين والمهاجمين تكنولوجيا عالية وحواسيب متطورة وانترنت ذو سرعة تدفق عالية.

إنّ اللجوء لمثل هذا النوع من التهديد الممنهج، يجعلنا نطرح الإشكالية التالية:

ماهي انعكاسات الاختراقات السيبرانية على سيادة الحكومات الالكترونية وأمنها المعلوماتي؟

وللإجابة على هذه الإشكالية، ارتأينا طرح بعض الأسئلة الفرعية المُساعدة للبحث:

1. ما هي الحكومة الالكترونية وفيما تتمثل أهميتها؟
2. ما هو الاختراق السيبراني وفيما تتحدد أشكاله؟

3. ما هي طبيعة الأمن السيبراني وماهي أبعاده ودوره؟
4. كيف يؤثر الاختراق السيبراني في سيادة الحكومات الالكترونية؟

لقد اعتمدنا في هذه الدراسة على بعض مناهج التحليل، محاولين بذلك الالمام بمختلف جوانب الموضوع: حيث اعتمدنا على بعض آليات المنهج التاريخي للعودة إلى أصل مصطلحات الدراسة: كالأمن، التهديد، الاختراق، العولمة، بالإضافة إلى بعض الأحداث التاريخية المهمة التي لها علاقة بالموضوع، أما المنهج الوصفي فقد اعتمدنا عليه لوصف مختلف الظواهر السياسية سالفة الذكر: كالتهديد والاختراق والأمن المعلوماتي وأنظمة الحماية، كلها تستوجب التحليل عن طريق الوصف الدقيق، وذلك بغرض تفسيرها من أجل الإجابة على الإشكالية المطروحة والتساؤلات الفرعية، وإثبات صحة الفرضيات.

انطلقنا من الفرضيات التالية:

1. تواجه الحكومات الالكترونية التهديدات السيبريانية بزيادة ارتباطها الوثيق بشبكات الانترنت مع ضعف أساليب الحماية من الاختراق.
2. تزيد الاختراقات السيبرانية للحكومات الالكترونية كلما زادت الثغرات الموجودة في قاعدة البيانات التي تسمح بذلك.
3. تتعرض الحكومات للانكشافية الأمنية وتتراجع سيادتها، كلما تعرضت لتهديدات لا تعرف وقتها أو مصدرها، خاصة بالنسبة للمؤسسات العسكرية، والأجهزة الحساسة المسؤولة عن أمن الدول.

أهداف هذا المقال العلمي يمكن إيجازها في النقاط التالية:

- يركز هذا المقال على الجانب المعرفي المتعدد التخصصات، فهو ينتمي للعلوم السياسية، لكنه يتحدث عن المجال التكنولوجي وأمن المعلومات، والهدف من ذلك محاولة تحديد انعكاسات التطور التكنولوجي على أمن الدول.
- حداثة الموضوع خاصة بالنسبة للحكومات الالكترونية في البلدان النامية.
- الوصول إلى معرفة هذا النوع الجديد من التهديدات العابر للقارات.
- محاولة الوصول إلى كيفية حماية الأنظمة المعلوماتية للحكومات الالكترونية، خاصة التي مازالت في بداية رقمنة قاعدة بياناتها.
- محاولة إيجاد حلول للتخفيف من تبعات العولمة على سيادة الدول.

ولتقسيم المقال من الناحية المنهجية، تمّ وضع المباحث التالية مع محاولة التطرق للجوانب المهمة للموضوع للإجابة على الإشكالية المطروحة:

- مفهوم الحكومة الالكترونية وأهميتها.
- الاختراق السيبراني: مفهومه، وأشكاله.
- أبعاد الأمن السيبراني ودوره في حماية الحكومة الالكترونية.
- تداعيات الاختراق السيبراني على سيادة الحكومة الالكترونية.
- تحقيق الأمن السيبراني لحماية السيادة بمفهومها الجديد

المبحث الأول

مفهوم الحكومة الالكترونية وأهميتها

خلال السنوات العشر الماضية بداية من القرن الحادي والعشرين، دخلت إلى قائمة المصطلحات المتداولة، عبارات عديدة أو تركيبات لفظية جديدة مثل: التجارة الإلكترونية، والتسويق الإلكتروني، والتعليم الإلكتروني، والبنوك الإلكترونية، وأيضاً الحكومة الإلكترونية. حيث تحمل هذه التركيبات اللفظية دلالة واضحة على استخدام تكنولوجيا المعلومات والاتصالات، في أداء أنشطة العمل الأساسية في المجال[1]، بالإضافة إلى إلمامها بكل جوانب الحياة اليومية للأفراد والدول، وهذا انعكاس لتبعات العولمة التي اجتاحت العالم ككل.

المطلب الأول: تعريف الحكومة الالكترونية

تعرف الحكومة الالكترونية بأنها: "قدرة القطاعات الحكومية على توفير الخدمات الحكومية التقليدية للمواطنين، وانجاز المعاملات عبر شبكة الانترنت بسرعة ودقة متناهيتين، وبتكاليف ومجهودات أقل ومن خلال موقع واحد على الشبكة"[2]، وتعرّف أيضا بأنّها: " عملية تغير وتحويل العلاقات من المؤسسات والمواطنين من خلال تكنولوجيا المعلومات والاتصال بهدف تقديم الأفضل للمواطنين وتمكينهم من الوصول إلى المعلومات، مما يوفر مزيد من الشفافية وتعظيم العائد وتخفيض النفقات"[3]، وفي تعريف آخر هي:" قدرة الأجهزة الحكومية على تبادل المعلومات فيما بينها من جهة، وتقديم الخدمات للمواطنين وقطاع الأعمال من جهة أخرى، وذلك بسرعة عالية وتكلفة منخفضة عبر شبكات الانترنت مع ضمان سرية وامن المعلومات المتناقلة في أي وقت وأي مكان"[4].

تتميز الحكومة الإلكترونية بتعدد تعاريفها الواسعة الاستخدام، مثل: الأعمال الإلكترونية، والإدارة الالكترونية والحكومة الرقمية، فمصطلح الحكومة الإلكترونية-E « Governmentيمثل شكلاً من أشكال الأعمال الإلكترونية E-Business ، الذي يشير إلى العمليات والهياكل التي تتفق مع إمداد الخدمات الإلكترونية للمواطنين، ومؤسسات الأعمال على حد سواء، ويمكن ملاحظة الحالة التي يحدث فيها التفاعل والتواصل الحالي مع الحكومة من خلال معاناة الطرف المتلقي للخدمة الحكومية، والمتمثلة في محدودية أوقات الاستقبال، والوقوف في طوابير انتظار طويلة للحصول على الخدمة المطلوبة، إلا أنه في الدول المتقدمة وبفضل تفعيل دور الحكومة الالكترونية، تتوفّرُ إمكانية تقديم الخدمات على مدار الساعة يومياً في كل أيام الأسبوع، بدون معاناة المواطنين ومؤسسات الأعمال في أماكن تواجدهم، يمكنهم حتى عدم الانتقال إلى المؤسسات الحكومية المقدمة للخدمات المطلوبة، وإذا بدأت الحكومة توظيف تكنولوجيا المعلومات والاتصالات الحديثة كوسائل الاتصالات السلكية واللاسلكية وشبكات المعلومات المحلية والإنترنت، بحيث يمكن لكل المواطنين أو مؤسسات الأعمال الاتصال بالحكومة من خلال شبكة الإنترنت، هناك فقط نكون أمام مجتمع مزدهر يلبي احتياجات المواطنين.[5]

وبالتالي فإن "الحكومة الإلكترونية" هي جزء من كيان إلكتروني أكبر، وهو مجتمع المعلومات والاتصالات والمعرفة، فكما يجب أن يتم تطوير المؤسسات الحكومية لتصبح إلكترونية، ينبغي أن يشهد المجتمع كله من مؤسسات خاصة ومؤسسات مجتمع مدني وأفراد نهضة إلكترونية، فالحكومة الإلكترونية تعني إذن تحولاً جذرياً في فلسفة الإدارة وتحقيق التناسق والتشبيك الإلكتروني بين القطاعات والمستويات الحكومية المختلفة، بحيث تنشأ قاعد بيانات وطنية مركزية شاملة، تضع أمام صانع السياسات العامة متخذ القرار صورة شاملة لأي نطاق من البيانات المتعلقة بسياسته العامة أو بقراره، كما تمكن هذه القاعدة المسؤول التنفيذي والباحث من دراسة القطاع الذي يهتم به وتطويره بالتنسيق مع القطاعات الأخرى ذات الصلة، وأخيراً تحقق الشفافية للإعلام والرأي العام، كما تمكن المواطن العادي الاستفادة من الخدمات الحكومية بسهولة[6].

وتعرّف منظمة التعاون الاقتصادي والتنمية مصطلح "الحكومة الإلكترونية" بأنه: استخدام تكنولوجيا المعلومات والاتصالات الجديدة من قبل الحكومات حسب تطبيقها على مجموعة كاملة من الوظائف الحكومية على وجه الخصوص، إمكانات التواصل التي توفرها

الإنترنت والتقنيات ذات الصلة لديها القدرة على تحويل هياكل وعمل الحكومة، وتعتبر الإدارة الفعالة لأمن المعلومات عاملاً رئيسياً حيث إن رغبة مختلف المستخدمين (المواطنين والأطراف الأخرى) في استخدام خدمات الحكومة الإلكترونية تعتمد بشكل كبير على الثقة التي يملكونها في أمان البيانات لهذه الخدمة[7].

كما أنّ الحكومة الإلكترونية هي تطبيق تكنولوجيا المعلومات والاتصالات، على الوظائف والإجراءات الحكومية وذلك بهدف زيادة الكفاءة والإنتاجية وضماناً لتحقيق مبدأ الشفافية ومشاركة المواطنين، هذا ما يُساهم في دعم وتطوير الحكم الرشيد[8]. فالشفافية في توفير المعلومات للمواطنين، يسمح لهم بالاطلاع التام على السير الحسن للمؤسسات، وبالتالي مسائلتهم من أجل مكافحة الفساد ومحاسبة المفسدين، وتحقيق مطالبهم دون اللجوء للعنف.

كما أنّ للبلديات تفاعل مباشر مع المواطنين، من أجل تلبية حقوقهم المدنية مثل: تسجيلات الأعمال، التسجيل التلقائي، التطوير الحقيقي وحتى اشراك الطفل في المدرسة، كل هذا يتطلب من المواطنين الاتصال بالبلدية والاحتكاك بالمصالح الحكومية التي تضمن لهم ذلك، ومن أجل تحسين الوظيفة الحيوية لهذه المؤسسة، تهدف الحكومة الإلكترونية إلى تكوين علاقة ديناميكية جديدة بين الحكومات والمواطنين حتى تُسهّل مشاركة المواطنين، من أجل تحقيق ذلك، ليس من المهم فقط إدخال التكنولوجيا في المهام التقليدية للبلدية، ولكن أيضًا في إدارة القطاع العام، حيث يكون المواطنون واحتياجاتهم هم النقطة المحورية لهذا الابتكار.[9]

المطلب الثاني: أهمية الحكومة الإلكترونية

- استخدام تكنولوجيا الإنترنت كمنصة لتبادل المعلومات، يعمل على توفير الخدمات، والتعامل مع المواطنين والشركات، وغيرها من القطاعات الحكومية. ويمكن أن تطبق الحكومة الإلكترونية من قبل السلطة التشريعية أو السلطة القضائية أو الإدارة، من أجل تحسين الكفاءة الداخلية وتقديم الخدمات العامة، وعمليات الحكم الديمقراطي.
- التوفير الإلكتروني للمعلومات الحكومية وخدماتها 24 ساعة في اليوم، سبعة أيام في الأسبوع، ممّا يقلل من البيروقراطية الحكومية، ويزيد من مشاركة المواطنين في الديمقراطية، ويعزز استجابة الوكالات لاحتياجات المواطنين[10].

- كما كان للزيادة الكبيرة في استخدام تكنولوجيا المعلومات والاتصالات على مدى السنوات القليلة الماضية تأثير كبير على مختلف جوانب المجتمع والأنشطة الاقتصادية من خلال جعل الإجراءات اليومية أسهل وأكثر كفاءة.
- يسمح التطبيق المناسب للحكومة الإلكترونية بمستويات أعلى من الفعالية والكفاءة في المهام الحكومية، وتحسين العمليات والإجراءات، وزيادة جودة الخدمات العامة، كما يحسن استخدام المعلومات في عمليات صنع القرار ويسمح بتحسين التواصل بين مكاتب حكومية مختلفة[11].
- تعتبر الحكومة جامع للمعلومات ومصدراً لها في نفس الوقت، ومقدمة للمعاملات والخدمات التي يحتاجها المواطنون من مؤسسات الأعمال، فيمكنها تحقيق هذا التصور من خلال ما يطلق عليه الحكومة الإلكترونية أو الرقمية المستخدمة لتكنولوجيا المعلومات والاتصالات المتقدمة، وبذلك تضمن أنماطاً وطرقاً جديدة وأساليباً مستحدثة تسهم في إمكانية الوصول للمعلومات، والمعاملات، والفرص، والخدمات.
- يتحقق دور الحكومة الالكترونية عند توفّر ثلاثة شروط أساسية وهي: المسائلة والشفافية والحكم الراشد، هذا ما ترتكز عليه الحكومة الالكترونية، التي جاءت بعد للوقاية من انتشار مختلف مظاهر الفساد الإداري والمالي في المجتمع ومؤسساته، ولتفعيل مقتضيات الإصلاح الإداري يجب على المؤسسات الحكومية الالتزام بنمط الشفافية والوضوح وإتاحة الوصول إلى المعلومات دون عراقيل تُذكر[12].

تراعي الحكومة الإلكترونية أولوية للخدمات التالية:

1. البيانات والوثائق وسجلات المعاملات الحكومية لكافة الخدمات التي تقدم للمواطنين.
2. التعليم، الخدمات الأكاديمية والتعليم الإلكتروني.
3. خدمات مؤسسات الأعمال والاستثمار.
4. الخدمات الاجتماعية.
5. السلامة العامة والأمن.
6. الضرائب.
7. الرعاية الصحية[13].
8. شؤون النقل.

9. الديمقراطية والمشاركة.
10. الخدمات المالية ووسائل الدفع[14].

المبحث الثاني
الاختراق السيبراني، مفهومه وأشكاله

ترتبط الهجمات السيبرانية بحدثين أساسيين، الأوّل هو استحداث أجهزة الكمبيوتر في منتصف الخمسينات من القرن الماضي، كوسيلة لمعالجة وحفظ المعلومات رقميا، ثم تطورت فيما بعد ليصبح جهاز الكمبيوتر أساسيا في عمل أغلب المؤسسات الخاصّة والعامّة، أما الحدث الثاني فهو ظهور الشبكة العنكبوتية الذي أحدث ثورة في التواصل ونقل المعلومات بسرعة فائقة، وفي سياق متّصل يرى البعض أن الثورة المعلوماتية تمثّل جيلاً ثالثا من الثورات التقنية بعد الثورة الزراعية والصناعية وبتسارع وتيرة استخدام الكمبيوتر لتحقيق التقدم في المجالين الأمني والعسكري، مع مطلع التسعينيات أطلق البعض مصطلح "الحرب السيبرانية الباردة Cyber cold war " أو"سباق التسلح السيبراني Cyber arms race"[15].

المطلب الأول: مفهوم الاختراق

1- نبذة عن تاريخ الاختراق:

في البداية لم تكن هذه الاختراقات والهجمات السيبرانية تستهدف الدول، بل كانت على شكل اختراقات على مستوى المؤسسات المالية والمصرفية، بالإضافة الى الشركات المتخصصة في برمجة نُظُم الاتصالات، ثمّ انتقلت هذه التهديدات لمستوى أكثر خطورة عبر الانترنت، من التهديد بالقتل لشخصيات سياسية إلى التهديد بتفجيرات في مراكز سياسية، لتصل في النهاية إلى إطلاق فيروسات هدفها إتلاف الأنظمة المعلوماتية في العالم[16]، وفي بحثنا هذا سنركز على ما تسبّبه هذه الاختراقات السيبرانية من أضرار كارثية للحكومات الالكترونية، حتّى أنها أصبحت تُشكل تهديدًا لسيادة الدّول في حدّ ذاتها.

وقد عُرف أوّل فيروس في أوائل الثمانينات عن طريق Arpanet والذي كان موجود قبل الانترنت، في 1988 تم اكتشاف أول دودة الكترونية "Computer warm"، حيث تم نشرها عبر آلاف الأجهزة الحاسوبية، عن طريق شخص يدعى Robert Timoris والذي أثار ضجة كبيرة في ذلك الوقت، وفي التسعينات تطورت التكنولوجيا عما كانت عليه لكن في نفس الوقت تطورت الفيروسات أيضاً، مثل: The Melissa والتي أحدثت أضراراً كبيرة في تلك

الفترة، حتى أنها دمّرت عدد كبير من الإيميلات عالميا، هذا ما استوجب التفكير في إنشاء مضادات للفيروسات، ومع حلول سنة 2000، أقدم مراهق عمره 15 سنة لُقِّب بـ : Mafia Boy على تنفيذ هجوم سيبراني على عدّة شركات ضخمة، منها: CNN, DELL, eBay, E- TRADE, Yahoo حيث كان Yahoo في تلك الفترة أكبر محرّك بحث في العالم، مما جعله يستقطب أكبر الاستثمارات في WALL st، وقد قام العديد من الخبراء التقنيين في هذه الشركات بتقييم حجم الخسائر التي تسبب فيها هذا الهجوم، فوجدوا أنها بلغت 1,2 بليون دولار، هذا ما جعل كبرى الشركات تبحث عن كيفية تحقيق أمنها السيبراني.[17]

2- تعريف الاختراق:

" هو الاستغلال المتعمّد لأنظمة الحاسب الآلي، والشبكات، والجهات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية؛ بهدف إحداث الأضرار"[18]، وفي تعريف آخر: "الاختراق الأمني هو أي حادث ينتج عنه وصول غير مصرح به إلى بيانات الحاسوب، أو التطبيقات، أو الشبكات، أو الأجهزة، كما ينتج عنه الوصول إلى المعلومات دون إذن، ويحدث عادةً عندما يتمكن المتسلل من تجاوز آليات الأمان"[19].

وفي العالم التقني يمكن تعريف الاختراق بأنّه: القدرة على الوصول إلى هدف تكنولوجي بطريقة غير مشروعة، عن طريق ثغرات لم يرها الشخص الذي تم اختراق حسابه في نظام الحماية الخاص بهذا الحساب، فيقوم المخترق من خلال تلك الثغرة بالتجسس ومن ثم سرقة المعلومات ونشرها للعامّة أو العبث بملكية الحساب بإزالة المسؤول المُباشر كما يحدث في بعض مواقع التواصل الاجتماعي والمواقع الالكترونية التابعة لمختلف المؤسسات وعلى وجه الخصوص الاقتصادية والحكومية، التي تتأثر كلاهما بالاختراق بصورة تعرّض أمن الدول للتلاعب والعبث المجهول الهوية، وإذا ما توفرت الإمكانات الفنية مع سرعة عالية للإنترنت، يستطيع المخترق تعطيل النظام لدى الهدف الذي اخترقه، أو تعديل مسار عمله بحذف أحد الملفات أو استبدالها بملف آخر، عندها يتحول وصف المخترق إلى مُخرّب «Cracker Hacker» كما أن الاختراق يكون في بيئة تختلف كل الاختلاف عن البيئة المعتادة، خاصّة فيما يتعلق بمحركات البحث والمتصفحات المستخدمة في الدخول، وتعرف هذه البيئة بالإنترنت العميق «The Deep Web» الذي يُمثّل أكثر من 90 % من الاستخدام الحقيقي لشبكة الانترنت[20].

المطلب الثاني: أشكال التهديدات الإلكترونية وأكثر الفئات المستهدفة

1. **الهجمات على السرية** (Confidentialité) **وسرقة الهوية**: تشمل سرقة معلومات التعريف الشخصية، والحسابات المصرفية، أو معلومات بطاقة الائتمان، حيث يقوم العديد من المهاجمين بسرقة المعلومات، ومن ثم بيعها على شبكة الإنترنت المظلمة "Dark Web"، لكي يشتريها الآخرون، للاستخدام غير الشرعي، وتُسمّى أيضا الهندسة الاجتماعية (Social engineering) وهي اختراق سيبراني، يعتمد على عملية التلاعب النفسي في أداء الأعمال، أو دفع الضحية للتخلي عن معلومات مهمّة سريّة، ويمكن اعتباره أسلوباً شائعا في عمليات الإرهاب النفسي[21].
2. **الهجمات على النزاهة** (Integrity): تتكون هذه الهجمات من التخريب الشخصي أو المؤسساتي، وغالبًا ما تسمى بالتسريبات، إذ يقوم المجرم الإلكتروني بالوصول إلى المعلومات الحساسة، ثم ينشرها بغرض كشف البيانات، والتأثير على الجمهور لإفقاد الثقة في تلك المؤسسة أو الشخصيّة، وهي نوع من التهديدات المستمرة المتقدّمة (Advanced Persistent Threats): تُعرف اختصارًا بـــ "APT"، حيث تستهدف النزاهة، يتسلل فيها مستخدم غير مصرّح به إلى شبكة غير مُكتشفة ويبقى فيها لفترة طويلة، القصد من APTهو سرقة البيانات، مع عدم الإضرار بالشبكة، وتحدث APTs في معظم الأحيان في القطاعات ذات المعلومات عالية القيمة، مثل الدفاع الوطني، ومؤسسات التصنيع، ومنصّات التمويل، وهذا ما يُشكّل تهديدا بالغ الخطورة على الأمن المعلوماتي للمنظومة الأمنية الدفاعية للدول.[22]
3. **الهجمات على التوافر**(Availability) : الهدف منها منع المستخدمين من الوصول إلى بياناتهم الخاصة، إلى أن يدفعوا رسومًا ماليّة معيّنة، ويتم استخدام البرامج الضارة والتجسّسيّة(Malware) ، كما تشير إلى برامج مصممة لانتزاع الوصول، أو إتلاف جهاز الحاسوب دون معرفة المالك وتتضمن الأنواع الشائعة من البرامج الضارة: برامج التجسس (spyware)، وkeyloggers، والفيروسات، وغيرها[23].
4. **تهديدات أمن الأجهزة المحمولة والثغرات الأمنية في الهواتف الذكية:** يمكن للمجرمين الإلكترونيين استغلال الثغرات الأمنية في الهاتف المحمول بسهولة للحصول على البيانات الخاصة، والتي تكون نتيجة تحميل تطبيقات الهاتف الذكي.

5. **اختراقات بيانات الرعاية الصحية:** في بداية 2015، واجهت شركة الرعاية الصحية "Anthem" اختراقًا كبيرًا للبيانات بواسطة متطفلين، وقد تأثر بذلك 78.8 مليون شخص، وتحتوي سجلات الرعاية الصحية على معلومات مهمة وحساسة تؤدي إلى سرقة الهوية من أجل الاحتيال على التأمين الصحي، مثل شراء الوصفات الطبية المزورة وبيعها.
6. **استهداف الأطفال من قبل المتحرشين الجنسيين:** يختبئ المستخدمون المتطلعون إلى استغلال الأطفال في أركان مظلمة عبر الإنترنت، للاتجار بصور الأطفال الخليعة غير القانونية. ويحدث ذلك عن طريق البريد الإلكتروني أو برامج نظير إلى نظير أو على نحو متزايد من خلال شبكة الويب المظلمة، وهي مساحة عبر الإنترنت لا يمكن الوصول إليها باستخدام محركات البحث القياسية. ومع أن هذه المواقع تعد مصدر قلق، فإنه من الأفضل تركها للمسؤولين في منظمات إنفاذ القانون، وعلى الشخص العادي تَجَنُّبها تمامًا[24].

المبحث الثالث

أبعاد الأمن السيبراني ودوره في حماية الحكومة الالكترونية

انطلاقاً من سنة 1982، ظهر هذا المصطلح بتصور غريب، صاغه كاتب الخيال العلمي ويليام جيبسون Gibdon William: "هلوسة جماعية يشترك فيها مليارات المشغلين يوميا، في كل دولة، كتمثيل للبيانات المستخلصة من بنوك المعلومات في جميع اجهزة الكمبيوتر في العالم "ولتسمية هذه الفكرة، جمع جيبسون كلمة "السبرنطيقا Cybernetics "التي تعني علم التحكم الآلي مع كلمة "الفضاء Space" وشكّل منهما مصطلح "الفضاء السيبراني " Cyberspace الذي أصبح حقيقة مع انتشار شبكة الإنترنت على كافّة أنحاء العالم، فالفضاء السيبراني Cyberspace إذن مصطلح حديث، ظهر نتيجة لثورة تكنولوجيا المعلومات ويشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الإنترنت العامة، فـ "الفضاء السيبراني" هو العالم المادي والمفاهيمي الذي توجد فيه جميع هذه الأنظمة[25].

أصبح يشكّل هذا الفضاء الافتراضي، ساحة المعركة التي تتقاتل فيها العديد من الأطراف سواء كانت تعرف بعضها البعض، أو كانت مجهولة فيما بينها، لذلك من الصعب معرفة هوية هؤلاء المتنافسين حول الهيمنة على البيانات الضخمة التي يحتويها هذا الفضاء السيبراني،

الذي لا يخضع لسيادة أي دولة[26]، ومع ذلك تسعى الولايات المتحدة الأمريكية الى القيام بدور كبير لفرض رقابتها وتحكمها على هذا الفضاء خوفا على أمنها القومي.

المطلب الأول: أهمية الفضاء السيبراني

يعتبر الفضاء السيبراني المجال المجازي لأنظمة الحاسوب والشبكات الإلكترونية، حيث تُخزّن المعلومات إلكترونيًا وتتم الاتصالات المباشرة على الشبكة، فهو عالم افتراضي غير مادّي يشمل: المعلومات الشخصية، والمعاملات الإلكترونية، والملكية الفكرية وغيرها من المواضيع.

تتلخص أهمية الفضاء السيبراني في النقاط التالية:

1) التفاعل الاجتماعي على نطاق واسع جدا، التواصل عن طريق الكتابة، القدرة على التسجيل ومنح القوة والقدرة على السيطرة على القدرات الكامنة لدى الإنسان.
2) في الفضاء السيبراني يمكن تبادل وتشارك الأفكار مع الآخرين والعمل على تطويرهم[27].
3) مرونة الوقت والفضاء السيبراني: حيث يتواصل الناس مع بعضهم البعض في نفس اللحظة.
4) التعددية المجتمعية: يمكن للمرء التواصل مع آلاف البشر من خلال إرسال رسالة على مدونة، ويستطيع أن يتلقى عدد لا حصر له من الرسائل من المستخدمين الآخرين، ويتواصل الناس من مختلف المجتمعات في لحظة.
5) المقدرة على التسجيل: يمكن حفظ المعلومات على شكل ملف (على الأقراص المدمجة، أو في شرائط).
6) السرعة في تبادل المعلومات: في الفضاء السيبراني من اليسير تنقّل المعلومات عبر مسافات ضخمة، باستطاعة البشر أن يرسلوا وأن يتلقوا رسائل في وقت وجيز جدا.
7) يتيح استخدام الشبكة الإلكترونية" السلطة والحرية"، حيث أن السلطة ترجع إلى التطوير الكامل للقدرات الكامنة للكائن البشري، مما يعني التحرر من الانحياز، الإرغام، العداوة، الشك في النفس، الافتقار إلى الفهم.
8) يتيح الفضاء الإلكتروني الفرصة للأفراد بأن يقدموا خبراتهم وأفكارهم لذلك، يلعب دورا هاما في تنمية الإبداع والشخصية.
9) المساواة: لا يتحيز الفضاء الإلكتروني أو يهمل الناس حسب الجنس، أو طبقتهم الاجتماعية أو العرق، فهو يمنح الناس الفرصة لأن يعرضوا أفكارهم الشخصية، وأن يبدعوا عن طريق مواقعهم الخاصة على الشبكة العنكبوتية العالمية.[28]

المطلب الثاني: فئات الأمن السيبراني

الأمن السيبراني هو ممارسة الدفاع عن أجهزة الحاسوب، والخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات من الهجمات الخبيثة، كما يُعرّف أيضًا باسم "أمن تكنولوجيا المعلومات"، أو أمن المعلومات الإلكترونية، وينطبق هذا المصطلح على مجموعة متنوعة من السياقات، بدءًا من قطاع الأعمال، وصولًا إلى الحوسبة المتنقلة، وبالإمكان عمومًا تقسيمها إلى عدّة فئات شائعة كما يلي:

1) **أمن الشبكات**: هو ممارسة تأمين شبكة الكمبيوتر من العناصر المتطفلة والانتهازية، سواء المهاجمين المستهدفين، أو البرامج الضارة.
2) **أمن التطبيقات**: يركز على الحفاظ على البرامج والأجهزة خالية من التهديدات، إذ يمكن أن يوفر التطبيق المخترق الوصول إلى البيانات المصممة للحماية، وإنّ تطبيق مفهوم الأمان الناجح يبدأ في مرحلة التصميم الأوّلي قبل نشر البرنامج أو الجهاز.
3) **أمن المعلومات**: يحمي سلامة وخصوصية البيانات، سواء في مرحلة التخزين أو التناقل.
4) **الأمن التشغيلي**: يشمل العمليات والقرارات التي تتعامل مع أصول البيانات، وتكفل حمايتها.

   إن الأذونات التي يمتلكها المستخدمون عند الوصول إلى الشبكة، والإجراءات التي تحدد كيف وأين يمكن تخزين البيانات أو مشاركتها، كلّها تقع تحت هذه المظلة.
5) **الاسترداد بعد الكوارث واستمرارية الأعمال**: يحدد كيفية استجابة المؤسسة لحادث أمان إلكتروني، أو أي حدث آخر يتسبب في فقدان البيانات، وهذا ينطوي على آلية عمل المؤسسة في استعادة بياناتها وعملياتها، للعودة إلى نفس القدرة التشغيلية التي كانت عليها قبل الحادث، وإنّ استمرارية العمل هي الخطة التي تعتمد عليها المنظمة بينما تحاول العمل بدون موارد معينة.
6) **تعليم أو تثقيف المستخدم النهائي**: أي التعامل مع عامل الأمن الإلكتروني الذي لا يمكن التنبؤ به وهو الأشخاص، إذ يمكن لأي شخص عن طريق الخطأ إدخال فيروس إلى نظام آمن ما، إنّ توجيه المستخدمين لحذف مرفقات البريد الإلكتروني المشبوهة، وعدم توصيل ذواكرUSB غير المعروفة، والعديد من الدروس المهمة الأخرى هو أمر حيوي لأمن أي منظمة.[29]

يُعدّ مفهوم "الأمن السيبراني" «Cyber security» أحد أهم مفاهيم الحقبة القادمة، التي ربما تشهد "حروبًا الكترونية" تحل محل الحروب التقليدية، لتصل إلى نفس مداها في الخسائر المادية، وربما تتعداه، في هذا الإطار يأتي كتاب "بيتر سيبنجر" الباحث المتخصص في السياسة الخارجية في مركز بروكينجز، و"آلان فريدمان" الباحث في معهد أبحاث الأمن السيبراني، ليستعرضا أبرز تحديات الأمن السيبراني، وكذلك تصاعد تأثيرات الحروب السيبرانية، بما في ذلك استغلال الجماعات الإرهابية لتكنولوجيا المعلومات الجديدة، لصالح أنشطتهم الإرهابية[30].

المطلب الثالث: أبعاد الأمن السيبراني

أ. **البعد العسكري**: كان المحيط العسكري هو الأول الذي بدأ فيه الانترنت بالانتشار بشكل رئيسي، بعدها توسع هذا المحيط ليشمل الجانب العلمي والأكاديمي، وبقيت تلك الأبحاث في بدايتها تخدم تحديث القدرات العسكرية وتطويرها، والإنجازات العلمية التي من شأنها اخلال التوازن في ميزان القوى الدولية، وبما أن التنافس بلغ ذروته في فترة الثمانينات بين الاتحاد السوفياتي والولايات المتحدة الأمريكية، ووصل حتى إلى التنافس في الوصول الى الفضاء الخارجي، وتطوير الأسلحة النووية، بدأت الأمثلة تزداد حول الاختراقات السيبرانية والهجومات التي طالت كل من: جورجيا واستونيا وكوريا الجنوبية وإيران، حتى انها كانت سببا في اندلاع صراعات مسلّحة مثلما حدث بين روسيا وجورجيا، كذلك ساد في تلك الفترة التشويش على الإدارات الحكومية، واختراقها لجعلها هشّة هذا ما سهّل بالتلاعب بها، مثلما حدث في الاختراقات السيبرانية التي وجّهت للمنشآت النووية في إيران هذا ما سبّب تهديدا للأمن القومي للدولة ككل، كما أن أهميّة المعلومات في الجانب العسكري تساهم في سرعة اتخاذ القرارات العسكرية وتحقيق الأهداف عن بُعد، لذلك وجب حمايتها من الاختراقات السيبرانية ومن الهجمات الالكترونية التي تسعى إلى تدمير قواعد البيانات وجعل الدول أكثر انكشافيه فيما يخص تهديدات العالم الخارجي[31].

ب. **البعد الاقتصادي**: أصبح الانترنت أساسا للمعاملات التجارية والمالية والاقتصادية، كما تستعمل الحواسيب في تسيير وتطوير الصناعات وتحريك الاقتصاد، وأصبح الكل مترابطا عبر شبكات الحاسوب، مما يستدعي الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي.

ج. **البعد الاجتماعي**: يفوق مستخدمي الانترنت 4 مليارات شخص في العالم، منهم أكثر من 6.2 مليار يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا لتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الانترنت، كما يعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة، وعليه فالبد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبيري في بعده الاجتماعي.

د. **البعد السياسي**: يعد التدخل الروس ي السيبراني في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن السيبيري في بعده السياسي، إضافة إلى التسريبات للوثائق الحساسة والاختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول، كما أن الفضاء السيبراني أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.

هـ. **البعد القانوني**: إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان الى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها. [32]

المبحث الرابع

تداعيات الاختراق السيبراني على سيادة الحكومة الالكترونية

انطلاقًا من إطار الأمن الدولي التقليدي، تطرّق الكاتبان للمفاهيم الأساسية التي يقوم عليها مصطلح "الأمن السيبراني"، مثل: "سيادة الدولة" التي تواجه تحديات جديدة تنبع من الأنشطة عبر الإنترنت، والتي يمكن ممارستها وتوجيهها عبر جميع أنحاء العالم بشكل غير منضبط، دون وجود إطار واضح لمساءلة الأفراد القائمين على هذه الأنشطة، كذلك يصعب في الفضاء الإلكتروني تمييز مبدأ "الحرب العادلة"، كما في الأنشطة المدنية والسياسية والعسكرية، ويوضح الكاتبان "بيتر سيبنجر" الباحث المتخصص في السياسة الخارجية في مركز بروكينجز، و"الآن فريدمان" الباحث في معهد أبحاث الأمن السيبراني، من خلال استخدام دراسات الحالة، كيف يتمكن المجرمون، وقراصنة الكمبيوتر، والحكومات، على حد سواء، من الاستفادة من نقاط الضعف البشرية والتقنية للوصول إلى أجهزة الكمبيوتر الأخرى، والقيام بهجمات سيبرانية [33]، فالخطأ البشري هو جزء رئيسي من اختراق أنظمة الأمن السيبراني، كما أن الخطأ الفردي يمكن أن يكون كافيًا لمنح فرص الوصول إلى شبكات بأكملها، بما في ذلك الحكومية، والصناعية،

والمؤسسات العسكرية، وذلك في الوقت الذي يصعب فيه تتبع أصول مُطوِّر البرمجيات الخبيثة أو الهجوم الإلكتروني المباشر، والكشف عن هويته[34].

المطلب الأول: خطورة الهجمات الالكترونية على الدول

زادت عمليات القرصنة التي تستهدف الحكومات الالكترونية للدول، خاصّة الموجهة ضد المنصات الرقمية الحكومية والتابعة لمؤسسات حسّاسة، أو العاملة في القطاع الخاص، فهي معرضة أكثر لهجمات محتملة، من قراصنة مجهولين أو موظفين من قبل دول تربطها مع دول أخرى نزاعات علنية أو خفية، ويمكن القول أن هناك علاقة منفعة علمية متبادلة بين الدراسات الأمنية ومصداقية الثنائية القائمة على المورد المعلوماتي والتحليل العلمي، في فك الشفرات الأمنية الدراسية المعقدة والتي توفرها الدراسات الاستخباراتية[35]، وتعتبر عملية الحفاظ على مصداقية المعلومات في العمل الاستخباراتي مهمّة جدا وحساسة، وذلك لضرورة حماية المعلومات السرية التي تخص أمن الدولة من أي هجمات سيبرانية مجهولة المصدر هدفها تهديد سيادة الدول.

ونظرا لزيادة التوتر في النظام الدولي ككل المعروف بفوضويته، وتوقع نمو الأنشطة الاستخباراتية والتجسس والتخريب، فضلا عن توتر العلاقات بين الدول المتنافسة اقتصاديا وعسكريا وتكنولوجيا، ارتقى تصنيف درجة مخاطر الهجمات السيبرانية التي تهدد مصالح الدول الى مرتبة المخاطر الجدية المتوقعة على المدى القريب، اذ ارتفعت وتيرة التهديد المتوقع من هجمات غير منظمة غايتها (التسلية الشخصية، وجني المال سابقاً)، لتصل اليوم الى مرحلة التخريب واختراق سيادة الدول، والإضرار بالأمن القومي ومصالح المؤسسات الالكترونية بمختلف مجالاتها وتخصصاتها، بل أصبح لهذه المعلومات آثار خطيرة على الهيئات الأمنية[36]، لذلك حمايتها تعتبر من أولويات الأجهزة الأمنية للدول[37].

أصبحت الحكومة الالكترونية في وقتنا الحاضر، تقوم على أساسيات التطور المعلوماتي والتكنولوجي، وبما أنّها أثبتت أهميتها بالنسبة للمواطن والدولة ككل، من تسريع وتيرة التنمية على مستوى المجتمع المدني، والقيام بمختلف الأدوار التي تمّ ذكرها سابقاً في أهمية الحكومة الالكترونية، أصبحت هذه الأخيرة وِجهة المخترقين للحصول على معلومات، أو دس معلومات مغالطة في الأنظمة المعلوماتية للمؤسسات الحيوية لدولة، وقد تطرقنا سابقاً لمختلف الأهداف التي يسعى إليها هؤلاء المخترقين، وفي هذا المحور سنتطرق إلى أهم التداعيات والانعكاسات، التي يتسبب فيها الاختراق السيبراني بمختلف أشكاله ولمختلف الأسباب المحرّكة له، على

الحكومة الالكترونية وما قد ينتج عن ذلك من مخاطر على الأمن المعلوماتي للدول ومنه، الأمن القومي ككل.

المطلب الثاني: العلاقة بين الأمن السيبراني والأمن القومي

تزداد العلاقة بينهما كلما زاد نقل المحتوى المعلوماتي والعسكري، والأمني، والفكري، والسياسي، والاجتماعي، والاقتصادي، والخدمي، والعلمي، والبحثي إلى الفضاء السيبراني، خاصة مع التسارع في تبني الحكومات الالكترونية والمدن الذكية في العديد من الدول، واتساع نطاق وعدد مستخدمي الانترنت في العالم، حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجي، اضافة الى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها،[38] هذا ما يجعلنا أمام شكل جديد من السيادة المقيّدة التي تتعرض للتهديدات السيبرانية والاختراقات من فضاء مجهول المعالم.

كما أن عدم معرفة الوجهة التي يأتي منها الهجوم، يجعل الحكومات الالكترونية في حالة ترقب دائم داخليا وخارجياً، فالتهديد لم يعد تقليديا كما كان سابقا، تتخذ الدول حذرها بالاستعدادات العسكرية وحماية الحدود، إنّ التهديد أصبح متغلغلاً في الدولة في حد ذاتها، ولذلك فالاختراقات المتكررة للمنظومة المعلوماتية للحكومات الالكترونية، تجعل الدول مكشوفة على العالم الخارجي، سواء للأعداء والمتربصين بها، أو للدول الأخرى عامّة فتصبح مادّة إعلامية دسمة تُباع عالميا بمبالغ معتبرة، كما أنها تفقد سمعتها ومصداقيتها داخليا وخارجيا، فيصبح المواطن في غنى عن خدماتها الالكترونية السريعة إذا كان سيفقدها بنفس السرعة، كذلك المؤسسات بمختلف مجالاتها ومستوياتها، لذلك فمن الضروري العمل على تحقيق أمن هذه الحكومات لما لها من انعكاس خطير على باقي المجالات التنموية والأمنية في حالة اختراقها سيبرانيا.

المبحث الخامس

تحقيق الأمن السيبراني لحماية السيادة بمفهومها الجديد

من التحديات الرئيسية التي تواجه خدمات الحكومة الإلكترونية هو كيفية الاستفادة من هذه التكنولوجيا الجديدة، ومواكبة العولمة ليس فقط من أجل تحسين كفاءة الإدارة العامة، ولكن أيضا لتعزيز الثقة في تدابير الخصوصية، من خلال الشفافية المتبادلة بين الإدارة العامة والمواطنين.

إنّ نظام إدارة أمن المعلومات هو:

- ضرورة فهم احتياجات أمن المعلومات في المنظمة.
- ضرورة وضع سياسات وأهداف، وتنفيذ عملية مراقبة وإدارة مخاطر أمن المعلومات التنظيمية، في ظل خلفية من المخاطر التجارية الشاملة.
- رصد واستعراض أداء وفعالية نظم الإدارة البيئية.
- التحسين المستمر على أساس القياسات الموضوعية.

لتحقيق أمن البيانات يجب توفير مجموعة من المتطلبات:

- **المصادقة:** القدرة على تحديد من يستخدم الخدمات (شخص أو برنامج).
- **التفويض:** القدرة على منح الحقوق للوصول إلى الموارد.
- **السرية:** القدرة على منع الوصول غير المصرح به إلى المعلومات.
- **النزاهة:** منع المعلومات من التعديل غير المصرح به، وضمان إمكانية الاعتماد عليها.
- **إمكانية التتبع:** القدرة على ربط أي معاملة مع شخص أو نظام قام بتنفيذ الإجراء بطريقة يمكن التحقق منها زمنياً.
- **عدم الإنكار:** القدرة على منع الشخص أو النظام المتدخلين في حدث أو إجراء لرفض مشاركتهم في الحدث أو تحديها[39].

في ظل مواجهة الهجمات الالكترونية المتزايدة الوتيرة وارتفاع حدة تأثيراتها، أصبح الاهتمام بعملية تحديد المصادر المستقلة والموثوقة والمعول عليها في غاية الأهمية، ويتزايد قلق القطاعين العام والخاص حيال طبيعة التهديدات بالجهوزية للتصدي للحوادث الإلكترونية والوقاية منها، وتتطلع بموثوقية والتحقيق فيها بمحترفين بارعين وتبادل المعرفة لكشف المهاجمين الإلكترونيين[40].

كما رصد فريق البحث في وحدة مكافحة التهديدات الإلكترونية لدى، "سيكيوروركس" عدّة حملات من محاولات الاختراق التي تحاول استغلال انشغال المستخدمين بجائحة وباء فيروس كورونا المستجدّ، وذلك من خلال تتبع بعض التقارير الصادرة عن أطراف مستقلة أو متابعة معلومات العملاء عن بعد، حيث وجد التقرير أدلة واضحة على محاولة اختراق تقف خلفها جهات متخصصة في الاختراق وجرائم المعلومات أو حتى جهات

حكومية في بعض الأحيان، بهدف استغلال انشغال الرأي العام بمتابعة مستجدات فيروس "كوفيد-19" وإغراء ضحاياها بزيارة روابط مشبوهة أو تشغيل ملفات برمجيات خبيثة.

ولاحظ فريق الباحثين، أن محاولات التسلل التي ترعاها بعض الجهات الحكومية تستخدم مستندات "أوفيس" تبدو مرتبطة بفيروس كورونا، كما أن الخبراء في الجرائم الإلكترونية الأكثر تطورا يستهدفون المؤسسات والبنى التحتية الحيوية في المناطق التي تضررت بشدة من جراء جائحة الوباء الصحي هذه، ولا تتغير أساسيات أسلوب العمل والسعي لجني مكاسب من محاولات الاختراق التي تُقدم عليها مجموعات الجريمة الإلكترونية بسبب هذه الجائحة العالمية، غير أن الخوف من المجهول، وعدم اليقين مما يحمله قادم الأيام، والتعطّش للبحث عن المعلومة يزيد من أعداد الضحايا المحتملين وبالتالي زيادة فرص نجاح هجمات الاختراق في بلوغ مبتغاها.

وينصح فريق من الباحثين، باتباع المؤسسات عدد من الإجراءات التي من شأنها المساعدة في الحد من أخطار هذه الهجمات، وهي:

1. تدريب الموظفين على كيفية التعرف على محاولات الاختيال والتصيّد الإلكتروني وآليات الإبلاغ عنها، فهذه المحاولات قد تلقى رواجا عبر البريد الإلكتروني، أو الهواتف، أو منصات التواصل الاجتماعي، أو الرسائل النصية القصيرة، أو غيرها من تطبيقات التراسل .
2. إجراء عمليات فحص منتظمة لأية نقاط ضعف محتملة، لاسيما البنى التحتية المتصلة بشبكة الإنترنت والتأكد من أن سيطرتهم على إدارة الأجهزة والتطبيقات، وتثبيتها عبر وسائط معروفة وموثوقة، والتحقق من إجراء عمليات الترقية والتحديث دوريا.
3. استخدام آليات التحقق من هوية المستخدم متعددة العوامل حيثما أمكن، فطلب عناصر إضافية للتحقق من الهوية يصعّب المهمة على من يقف خلف محاولات الاختراق باستخدام معلومات مسروقة من المستخدمين .
4. تطبيق ضوابط رصد للأنشطة المشبوهة عبر الشبكة وعلى النقاط الطرفية، والتركيز على رصد والتحقق من أي نشاط غير معتاد للملفات المستخدمة في محاولات الاختراق باستخدام أدوات مثل: *PowerShell* ، *أو WMI* ، *أو WScript* ، أو أي اتصال غير معتاد عبر الشبكة .

5. إلزام المستخدمين بالاتصال عبر موارد الشركة مثل الشبكات الافتراضية الخاصة وأنظمة خادم النطاق (DNS) عند الحاجة للاتصال بشبكة الإنترنت، فهذه المنهجية توفّر فرص مراقبة إضافية في حال نجاح محاولات اختراق نقطة اتصال المستخدم.[41]
6. التركيز على متطلبات الأمان للمؤسسة عند تحديد أداة عقد المؤتمرات عن بعد والشركات التي تقدمها، وذلك للتأكد من أن الأداة تسمح بالحفاظ على مستوى الحماية اللازم للمحادثات والبيانات .
7. تقديم الإرشادات للموظفين حول طرق الاستخدام السليم لخدمات المؤتمرات عن بعد، واستخدام مزايا التحقق من هوية المستخدم مثل كلمات المرور وغيرها من المزايا المتاحة، وتجنّب الإفصاح عن مضمون الاجتماعات للعلن.
8. مراجعة خطط الاستجابة لحوادث الاختراق والتأكد من أنها لا تزال مناسبة لبيئة العمل بعد هذه التغييرات، إذ يجب التفكير في كيفية اختبار هذه الخطط دون أن يتسبب ذلك في مزيد من الضغوط غير الضرورية على المؤسسة .
9. اختيار مزود خدمة يقدم قائمة متكاملة من خيارات تتبع التهديدات، أو يتيح خيارات مكمّلة لها، وقادر على توفير الدعم اللازم لنموذج التعامل مع التهديدات لدى المؤسسة، وهو ما يساعد في الحد من احتمال أن يضيع فريق الأمن الداخلي ساعات من الوقت في تتبع خيوط معلومات غير دقيقة[42].

الخاتمة:

يعتبر الاختراق السيبراني من المعيقات البالغة الخطورة، التي تعيق الأداء الجيد والفعّال للحكومات الالكترونية، إن العمل على تطبيق الحكومة الالكترونية وإدخال ما يستجد في مجال التقنية إلى بيئة العمل دفع إلى رفع مستوى الأداء، كما أن التطوير الإداري الذي يهدف إلى رفع كفاءة الأداء من خلال التغيير والتحديث في الجوانب الإدارية المختلفة يهتم بشكل كبير بالتقنية واستخدامها في مجال عمل الحكومة الالكترونية وذلك لما للتقنية من دور في رفع كفاءة الأداء وسرعة الانجاز وخفض التكاليف.

لكن إذا كانت الاختراقات السيبرانية تعمل على ضرب أهداف الحكومة الالكترونية من حفظ لخصوصية البيانات وتحقيق أمنها، فإن هذا التهديد اللاّتماثلي يأخذنا الى ضرورة اتخاذ إجراءات وتدابير وقائية، تمنع وقوع هذه الاضرار الفادحة على المؤسسات الحكومية الالكترونية، ومنه تتحقق حماية سيادة هذه الحكومات من كل أنواع التهديد السيبراني

والاختراق والهجوم، ومن هذه التدابير لا بد لنا من ذكر أهم النقاط التي تطرقت إليها هذه الدراسة:

1. الاعتماد على أجهزة حديثة عالية التقنية، مزودة بأحدث برمجيات الحماية ضد الاختراقات السيبرانية.
2. الاستعانة بالخبراء والتقنيين المدربين بشكل احترافي، من أجل الترصد لعمليات الاختراق في أسرع وقت لتجنب حدوث خسائر أو تقليلها.
3. تكوين مكثف لجميع الموارد البشرية خاصة العاملة في الأجهزة الحساسة للدولة، من أجل تحقيق الأمن السيبراني، وذلك لتقليل حدوث الأخطاء.
4. القيام بعمليات التحقيق والترصد الدورية للبحث عن أية ثغرات أمنية من شأنها أن تكون سببا لولوج القراصنة لأنظمة الحماية وتعطيلها.

الهوامش:

1 رأفت رضوان، الحكومة الالكترونية، المركز الدولي للدراسات الدولية والاستراتيجية، العدد 5، 2005، ص 14.

2 سناء الدويكات، مفهوم الحكومة الإلكترونية وأهدافها، *https://mawdoo3.com/* ، تاريخ النشر: 2017/10/11، تاريخ الاطلاع: 21-09-2023 19:35.

3 بن عدة أمحمد، طيراوي دومة عمي، برنامج الحكومة الإلكترونية المتكاملة وسبل تطبيقيا في الجزائر بالاعتماد على التجربة القطرية، مجلة الدراسات الاقتصادية المعاصرة، المجلد 3، العدد 06،2018، ص5.

4 مطاي عبد القادر وبن شنينة كريمة، واقع ومتطلبات إرساء الحكومة الالكترونية في الجزائر، مجلّة التكامل الاقتصادي، المجلد 07، العدد 02، جوان 2019، ص 179.

5 سحر قدوري الرفاعي، الحكومة الالكترونية وسبل تطبيقها: مدخل استراتيجي، مجلة اقتصاديات شمال إفريقيا، العدد 07، ص 308.

6 رأفت رضوان، مرجع سابق الذكر، ص 08.

7 Hector D. Puyosa P, e-Government: Security Threats, posted on Aug 25, 2013, 7:29 PM, date of view: 20/04/2020 , http://stc-egov.ieee.net/blog/

8 Organisation of American State, What is e-Government?, Date of view: 02/06/2020, http://portal.oas.org/Portal/Sector/SAP/Departamentoparala

9 المرجع نفسه.

10 What is Electronic Government (e-Government) ; https://www.igi-global.com/dictionary/investigating-enterprise-

11 Organisation of American State, What is e-Government? ; ibid.

12 سحر قدوري الرفاعي، مرجع سابق الذكر، ص 309.
13 رأفت رضوان، مرجع سابق الذكر، ص 18.
14 المرجع نفسه.
15 علاء الدين فرحات، مرجع سابق الذكر، ص 91.
16 علاء الدين فرحات، مرجع سابق الذكر، ص 91.
17 مدخل تاريخي لأمن المعلومات، مؤسسة إدراك، تاريخ النشر: 2019، تاريخ الاطلاع: 19-06-2020 17:58 *https://courses.edraak.org/courses/course*.
18 المركز الوطني الارشادي للأمن السيبراني، ما هو الهجوم السيبراني؟، تاريخ النشر: 16-02-2020، تاريخ الاطلاع: 21-09-2023 20:07، *https://cert.gov.sa/ar/awareness/whatiscyberattack*
19 ما هو الاختراق الأمني؟، تاريخ الاطلاع: 21-09-2023 20:21، *https://me.kaspersky.com/resource-center/threats/what-is-a-security-breach*.
20 ندى الحارثي، الأمن السيبراني وطرق الحماية من الاختراق، الوطن، تاريخ النشر: 2019/04/06، تاريخ الاطلاع: 19-06-2020 17:58، *https://www.alwatan.com.sa/article/1004708*
21 سعيد عطا الله، ما هو الأمن السيبراني وما فوائد الأمن السيبراني، تاريخ النشر: 2020/05/14، تاريخ الاطلاع: 2020/06/20 10:41، *https://www.arageek.com/l/%d9%85%d8%a7-* .
22 المرجع نفسه.
23 المرجع نفسه.
24 أهم 7 تهديدات إلكترونية يجب التنبه لها في عامَي، تاريخ الاطلاع: 2020/05/22، *https://me.kaspersky.com/resource-center/threats/top-7-cyberthreats*
25 علاء الدين فرحات، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلّة العلوم القانونية والسياسية، المجلد 10، العدد 03، ديسمبر 2019، ص 90.
26 إيليوت كوهين، العصا الغليظة: حدود القوة الناعمة حتمية القوة العسكرية، ت: فواز زعرور، بيروت: دار الكتاب العربي، 2018، ص 223.
27 نجوى السودة، مؤتمر حروب الفضاء السيبراني، بحث الفضاء السيبراني، تاريخ النشر: 15/ 05/ 2015، تاريخ الاطلاع: 2020/04/20، *https://seconf.wordpress.com/2015/05/15/%*
28 نجوى السودة، مرجع سابق الذكر.
29 سعيد عطا الله، مرجع سابق الذكر.
30 نجوى السودة، مرجع سابق الذكر.
31 بارة سمير، مرجع سابق الذكر، ص260.

32 إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلّة العلوم القانونية والسياسية، المجلد 10، العدد 01، 04/ 2019، ص 1023.

33 بيتر سيبنجر والآن فريدمان، كيف سيواجه العالم تحديات "الأمن السيبراني" ؟، تاريخ النشر: 24-09-2014، تاريخ الاطلاع: 21-09-2023 20:47، *https://www.siyassa.org.eg/News/4925*

34 نجوى السودة، مرجع سابق الذكر.

35 بلهول نسيم، الدراسات الأمنية المعقدة المفاهيم والمقاربات، ط 1، عمان: دار الحامد للنشر والتوزيع، 2019، ص 166.

36 المرجع نفسه، ص 171.

37 زيادة تهديدات الاختراق الالكتروني للمؤسسات الخليجية الحساسة، مركز الشرق الأوسط لاستشارات السياسية والاستراتيجية، تاريخ النشر: 2019/11/13، تاريخ الاطلاع: 2020/06/04، https://www.*menaccenter.com/2019/11/13/%D8%B2%D* -

38 إسماعيل زروقة، مرجع سابق الذكر، ص 1025.

39 Hector D. Puyosa، ibid.

40 جون إس ديفيس الثاني وآخرون، تهديدات مجهولة المصدر نحو مساءلة دولية في الفضاء الالكتروني، مؤسسة *Rand، 2017، https://www.rand.org/content/dam/rand/pubs/research_*

41 هبة السيد، 9 إجراءات تتيح للمؤسسات التصدي للهجات الإلكترونية بسبب فيروس كورونا، مجلة اليوم السابع، تاريخ النشر: 16/04/ 2020 01:46، تاريخ الاطلاع: 2020/05/15، https://*www.youm7.com/story/2020/4/16/*

42 هبة السيد، المرجع نفسه.