التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

الألعاب الإلكترونية بيد الإرهابيين أداة للتجنيد

إعداد: إدارة الدراسات والبحوث

قضايا الإرهاب 3
مارس 2023

قضايا الإرهاب

إصدار شهري يصدر عن التحالف الإسلامي العسكري لمحاربة الإرهاب

المشرف العام

اللواء الطيار الركن محمد بن سعيد المغيدي

الأمين العام للتحالف الإسلامي العسكري لمحاربة الإرهاب / المكلّف

رئيس التحرير

عاشور بن إبراهيم الجهني

مدير إدارة الدراسات والبحوث

الألعاب الإلكترونية بيد الإرهابيين
أداة للتجنيد

إعداد: إدارة الدراسات والبحوث

شهد العالم خلال القرن الماضي ثورة معلوماتية وتقنية متسارعة، مما اسهم بشكل سريع وملحوظ في تطور الخدمات الإلكترونية بكافة أشكالها وفي جميع القطاعات سواءً أكانت في القطاع الحكومي أم في القطاع الخاص، كما ساهمت بتغيير أنماط الحياة للمجتمعات، ابتداءً من العادات والممارسات والسلوك وصولاً إلى سلم القيم وأنماط الحياة، مما أدى إلى التخلي عن العديد من القيم والعادات الإجتماعية التي كانت مغروسة في مجتمعاتنا، فتواجه التنشئة الاجتماعية مجموعة من المؤثرات التي تؤثر في تنشئة الأجيال، وكان للثقافة الإلكترونية دور كبير في تشكيل القيم وتكوين الهويات الثقافية والحضارية.

ولا ننسى أن العالم أصبح قرية صغيرة في ظل اتصاله بشبكة الإنترنت بشكل دائم، لذا بات من الضروري لكل دولة حماية أفرادها ومؤسساتها ومقدراتها وحضارتها من آثار هذا الانفتاح اللامحدود للإنترنت، وإدراك الجميع اليوم لفوائد تقنية المعلومات. ولكن في الوقت نفسه نيقن أن هنالك العديد من المخاطر الكامنة في تغلغل هذه التقنية بين أفراد المجتمع، حيث يتطلب من المجتمع والمؤسسات الحكومية الحيلولة دون الوقوع في تلك المخاطر والحد منها.

أدى الانتشار الواسع للألعاب الإلكترونية إلى صقل شخصية الأطفال والشباب بانتهاجهم لقيم واتجاهات فكرية وسلوكية متنوعة من خلال ما يتم تعلمه من خلال تلك الألعاب، حيث أصبحت هذه الالعاب تنافس دور الأسرة في بناء الفكر وتكوين الشخصية للاعبين مما أدى إلى ظهور تنشئة اجتماعية لا تتوافق مع العادات والتقاليد المتبعة في المجتمع.[1]

كما يجب ألا ننكر بأنها حقيقية نعيشها في مجتمعاتنا، وتشكل مصدرًا مهمًا من مصادر التنشئة الاجتماعية لما لها من تأثير

مباشر على سلوكيات الأفراد والمجتمعات، لذا يجب الانتباه للأوقات التي يقضيها الأطفال والشباب مع هذه الألعاب[2].

وفي ظل الدور الذي تعلبه الألعاب الإلكترونية نلاحظ أن مهمة تجنيد الأطفال والشباب سهلة لدى الجماعات الإرهابية لأنهم لا يمتلكون الثقافة العالية التي تميز بين الفكر الصحيح والفكر التكفيري المتطرف فيسهل عليهم إقناعهم وبناء أفكار خاطئة وزرع مفاهيم ومعتقدات مغلوطة تسهم باستقطابهم عن طريق الألعاب الإلكترونية التي تُبث لهم، كون ممارسة الألعاب الإلكترونية التي تحتوي على حروب، وتفجيرات، وقتل، وتدمير، وعنف، وإرهاب تؤثر بشكل مباشر على الأطفال والشباب كونها تسهم في البرمجة الذهنية لديهم، فتصبح هذه المشاهد طبيعية بالنسبة لهم بل يتحمسوا لتطبيقها.

لذا سعت العديد من الدول إلى اتخاذ التدابير والاحترازات لمواجهة الإرهاب الإلكتروني إلا أن هذه الجهود تحتاج للمزيد من الإجراءات والتدابير لمواجهة هذا السلاح الخطير لتنوع مصادره، وأبعاده، وأغراضه. ويمكن القول أن الإرهاب الإلكتروني هو إرهاب المستقبل وهو الخطر القادم نظراً لتعدد أشكاله وتنوع أساليبه وتعدد مجالاته بإبتكار طرق حديثة لمواجهته.

الإرهاب الإلكتروني

ظهر مصطلح الإرهاب الإلكتروني في ثمانينيات القرن الماضي، واقتصر تناول ذلك المصطلح على الإشارة لتلك الهجمات التي يستخدم فيها الكمبيوتر ضد اقتصاد وحكومات الدول، ثم اتسع هذا المفهوم مع بداية عقد التسعينيات حيث شهد نموًا متزايدًا للإنترنت واستخدامه بشكل واضح في الربيع العربي، وما كان له من أهميه في حركة العلاقات الدولية.

مفهوم الإرهاب الإلكتروني

لا يوجد تعريف موحد للإرهاب الإلكتروني حيث يوجد العديد من التعريفات له، فظاهرة الإرهاب الإلكتروني أو الرقمي (Cyber Terrorism) هو مصطلح يشير إلى ثقافة سلبية ونوعًا أخر من الإرهاب نتيجة التطور التكنولوجي والثورة المعلوماتية، حيث يتم استغلال شبكة الإنترنت وأدوات التقنية للهدم والتخريب والسرقة.

الإرهاب الالكتروني يعني العدوان أو التخويف أو التهديد ماديًا أو معنويًا باستخدام الوسائل الإلكترونية الصادرة عن الدول أو الجماعات أو الأفراد عبر الفضاء الإلكتروني، أو أن يكون هدفًا لذلك العدوان بما يؤثر على الاستخدام السلمي له[3]

ويُعرّف أيضاً الإرهاب الإلكتروني بأنه استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية، أو اقتصادية، أو اجتماعية، أو عرقية، أو مذهبية، أو فكرية.

كما يُعرّف الإرهاب الإلكتروني بالعدوان أو التخويف أو التهديد ماديًا أو معنويًا باستخدام الوسائل والأدوات الإلكترونية من الدول، أو الجماعات، أو الأفراد على الإنسان باستهداف دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صور الإفساد في الأرض[4].

أشكال الإرهاب الإلكتروني

يمكن حصر أشكال الإرهاب الإلكتروني كالآتي: [5]

- استغلال المنصات الإلكترونية من الإرهابيين للتواصل والتنسيق مع أعوانهم ومموليهم وتوجيهها لأوامر لهم عبر شبكة الأنترنت لتنفيذ عمليات إرهابية.

- إنشاء مواقع مخصصة لشن حملات إعلامية على الدول التي تقوم بترويعها، حيث تعرض صور الرهائن والأسرى وإعدامهم، أو تثير الإشاعات التي تهدف إلى زعزعة أمن واقتصاد البلد أو الجماعة المستهدفة، أو تنظيم المظاهرات والأعمال التخريبية التي توجه للبلد المستهدف.

-الاختراق لمجرد العبث والتخريب، حيث تشير الدراسات النفسية لشخصيات هؤلاء المخترقين إلى وجود أمراض نفسية لديهم تدفعهم إلى الثورة على المجتمع أو المؤسسات مما يدفعهم إلى العبث والتخريب.

-الاستيلاء على أموال الآخرين أو ملفاتهم الشخصية، واختراق جهاز حاسب آلي تعود ملكيته لفرد، حيث يعد ذلك سطواً على ممتلكاته الخاصة، واستخدام أدوات التقنية الحديثة في الحصول على معلومات خاصة للأفراد أو المؤسسات وابتزازهم بتهديدهم بنشرها على الشبكة إن لم يستجيبوا لمطالبهم.

- التلقين الإلكتروني وذلك بحشد المؤيدين والمتعاطفين معهم، وبمبادئهم وطرقهم ووسائلهم في محاولة لتعبئة وتجنيد إرهابيين جدد عبر منصات التواصل الاجتماعي وغرف الدردشة في الألعاب الإلكترونية.

الألعاب الإلكترونية

تعود نشأت الألعاب الإلكترونية إلى بدايات صناعة الحاسب الآلي، حيث اعتمدت هذه الألعاب على الإمكانات البرمجية المتوفرة في محاكاة الواقع الحقيقي والافتراضي بعناصره ومؤثراته المختلفة، مما فتح مجالات تفاعلية واسعة أمام الإنسان للتعليم والترفيه والتسلية، وهو ما دفع الشركات المختصة إلى تطوير أجهزة وبرمجيات هذه الألعاب، من اجل الرقي بالوعي الثقافي والاجتماعي.

ولقد شهدنا في السنوات الأخيرة انتشار واسع لأماكن بيع الألعاب الإلكترونية ومراكز وصالات الألعاب بشكل كبير بمختلف أشكالها وأحجامها وأنواعها، وقابل هذا الانتشار وجود طلب متزايد من قبل الأطفال والشباب على اقتناء هذه الألعاب، وانتشرت هذه الأجهزة والألعاب الإلكترونية في المنازل والنوادي ومراكز الألعاب وغالباً ما تعتمد تلك الألعاب على سرعة الانتباه والتركيز والتفكير.[6]

ومع تطور الأجهزة الإلكترونية وازدياد عددها توسعت الألعاب المرتبطة بها، فبدأت بتسلسل تكتيكي بدءًا من ألعاب السرعة والإثارة مثل سباق السيارات ثم الصراع بين الحيوانات وصولاً إلى الحروب بين الدول والعصابات والميليشيات لتشتمل على تكتيكات عسكرية واستخدام معدات عسكرية خفيفة وثقيلة مثل الألعاب الحربية والعسكرية ألعاب التدمير والقتل والسرقة والنهب فأصبحت الألعاب الإلكترونية مع التقدم التكنولوجي المتسارع تلقى

ترحيب وقبول من اللاعبين على اختلاف الفئات العمرية لما تحتوية من إثارة وتشويق.

وفي الوقت نفسة أصبحت الألعاب الآن خارجة عن السيطرة فتعدت بأن يشارك الأطفال والشباب في صناعتها أو برمجتها، بل وصلت إلى أن تغرس فيهم مضمون اجتماعي معين ربما على حساب المضمون الاجتماعي لمجتمعاتنا، الأمر الذي قد يفقد الطفل ولاءه لمجتمعه ويضعف روابطه به، وقد يتعدى الأمر إلى أن هذه الألعاب الإلكترونية قد تقدم مضامين اجتماعية منحرفة تسهم في أن يصبحوا أعداء حقيقيين لوطنهم.[7]

أنواع الألعاب الإلكترونية.

هناك العديد من الأنواع للالعاب الإلكترونية وتنقسم كالآتي:

- ألعاب تعتمد على قصة أو شخصية كرتونية وهذا النوع من الألعاب مفيد جدًا.

- ألعاب فكرية تعتمد على الخيال وسرعة البديهة والذاكرة والنشاط الذهني.

-الألعاب التي تعتمد على إستراتيجية حربية تحتاج إلى وضع خطط، وهذا يعد نوع من المراحل المتقدمة والتي تحتاج إلى نضج عقلي.

- ألعاب تعتمد فقط على صراع البقاء وهذا النوع يكون عنيفًا ولكنه يؤدي لتبلد الذهن والفكر إذ أنه يعتمد على القتل والتدمير والتخريب والنشوة [8]

تكمن الخطورة في انتشار الألعاب الإلكترونية بعدم وجود قانون يمنع بيعها للأطفال، وأن بعضهم يقومون بتحميل تلك الألعاب من الإنترنت عن طريق مواقع أجنبية، أو عربية بطريقة غير قانونية، وكذلك يقومون بتطوير اللعبة ليكون فيها تخطيط إستراتيجي مبني على تعاون بين مجموعة من اللاعبين على سرقة بنك أو متجر وكذلك لبس الأقنعة وإخفاء الشخصيات والتشجيع على القتل وسلب أموال الناس وممتلكاتهم وعدم احترام قوانين الأمن وأنظمته.

إن الوجه السلبي للألعاب الإلكترونية، يتمثل أساسًا في خطورة المواضيع التي تتناولها مثل العنف والجنس وتجاهل الآخر، ذلك أن القليل فقط من هذه الألعاب يتم تصميمها لأغراض التسلية المثقفة غير المؤذية أو لغايات تعليمية تثقيفية محددة، في حين تعمل تصميمات الألعاب الأخرى على تنميط الحاجات الترفيهية للناشئة، وتتسابق في تحويل الرذائل الافتراضية من قتل وعنف وتحايل وكذب إلى منتجات ترفيهية ذات جاذبية عالية تستهدف فئات عمرية لا تملك وسائل مقاومة هذه التهديدات لضعف وعيها وإدراكها لأنها مازالت في المراحل الأولى من التلقي والتكوين.[9]

العنف في الألعاب الإلكترونية وعلاقته بالإرهاب الإلكتروني

نجد أن الكثير من الألعاب الإلكترونية تحتوى على نماذج مختلفة من الشخصيات والسلوكيات العنيفة المكررة التي يتقمصها الأطفال والشباب دون إبداء أي شكل من أشكال النقد والإدانة التي قد تحافظ على بقاء الرأي الاجتماعي الغالب الذي يرى في العنف سلوكًا اجتماعيًا مستهجنًا من الواجب صده ومقاومته.

ويتزامن ذلك مع الغياب الملحوظ لدور الأسرة في السيطرة فيما يتعلق بالرقابة على الألعاب الإلكترونية وظهور طبقات اجتماعية جديدة أساسها فارق الاستخدام المعلوماتي والوعي بالمخاطر المحتملة، خاصة إذا ما أخذنا في عين الاعتبار مستوى الوعي الثقافي لدى فئات كثيرة من المجتمع، وهو ما يقلل من الإحساس بمخاطر الألعاب الإلكترونية بصورة عامة.[10]

إن ما تجلبه الألعاب الإلكترونية التي تروج لها المنظمات الإرهابية ما هو الا عملية تجنيد منظمة للأطفال والشباب، فمعظم الألعاب الإلكترونية تأخذ أشكالاً وأنواعاً مختلفة من البنادق والمسدسات والخناجر والسيوف والسرقة والتدمير والاستيلاء على أموال وممتلكات الآخرين وبث الرعب والخوف في نفوس الآخرين، وهذه الأفعال تدمر فطرة الأطفال والناشئة السوية والبعيدة كل البعد عن بيئته وتحوله إلى بيئة تشجع على العنف والقتل والتدمير وكراهية الآخرين[11]. وتزيد من التعصب الطائفي والمذهبي، وتنشئ الأطفال على عدم احترام قواعد وأنظمة الأمن، وضعف المسؤولية الاجتماعية، وكلها قيم مناهضة للمواطنة الصالحة .

لم يعد ضرر بعض الألعاب الإلكترونية ينحصر في العنف الموجود داخل عالمها بل يصل إلى تضليل الشباب للالتحاق بالمنظمات الإرهابية، حيث يتواصل أعضاء المنظمات صوتيًا بين بعضهم البعض مع اللاعبين في عالم الألعاب الإلكترونية عبر الإنترنت للتلاعب بأفكارهم ومحاولة تضليلهم، كما أُستخدمت بعض الألعاب الإلكترونية للتواصل بين الأعضاء في الجماعات الإرهابية لتنفيذ عمليات إرهابية حيث

ينضم الأعضاء إلى معركة إلكترونية افتراضية في إحدى الألعاب ويقومون بالتخطيط والتواصل في ذلك العالم بعيدًا عن أعين المراقبة المباشرة ذلك أن الأجهزة الخادمة لتلك الألعاب موزعة في جميع أنحاء العالم، وتحاول التنظيمات الاتصال باللاعبين بطرق مختلفة مثل الدردشة صوتيًا أو نصيًا ومحاولة تضليلهم، وليس من البعيد أن يتأثر الأطفال والمراهقين بذلك ويتمنوا تجربة ما يحدث في عالم الألعاب الإلكترونية العنيفة خارج منازلهم، الأمر الذي يترجم باستدراجهم ووقوعهم ضحايا لهذه المحاولات.

السلوك العدواني في الألعاب الإلكترونية وعلاقته بالإرهاب الإلكتروني

إن ممارسة الأطفال للألعاب الإلكترونية التي تعتمد على العنف يمكن أن تزيد من الأفكار والسلوكيات والعدوانية عند الأطفال والشباب، وأن هذه الألعاب قد تكون أكثر ضررًا من أفلام العنف في التليفزيون أو السينما لأنها تتصف بصفة التفاعلية بينها وبين الطفل وتتطلب من الطفل أن يتقمص الشخصية العدوانية والتي تغرس في نفوس الأطفال أن القتل شيء مقبول وممتع.

إن مخاطر الألعاب الإلكترونية العنيفة تكمن في التعزيز المتواصل لسلوك القتل والتدمير وغير ذلك من الممارسات العدوانية، بحيث يكون الفوز في اللعبة مشروطاً بممارسة قدر أكبر من التدمير وسفك الدماء، ويتم ذلك عن طريق تعليم اللاعب سبل الولاء الكامل والاندماج الكلي في زمن ومكان اللعبة الافتراضي يدفعه بعد ذلك إلى ممارسة الحلول العنيفة المتاحة عند تعامله مع الأشخاص واجتيازه للعقبات والعراقيل التي تقف حائلا أمام حصوله على العدد المطلوب من النقاط للوصول إلى المراتب النهائية في اللعب. حيث تسند المكافآت والحوافز مقابل عمليات القتل والتدمير التي تمتد طيلة زمن اللعبة، فيجد الطفل نفسه وسط دائرة مغلقة من أفعال العنف والسلوك العدواني، وردود الأفعال التي تبارك هذا السلوك، وتجزل العطاء لكل من ينجح في القيام به، أي أن الشخص الذي يجيد استعمال العنف والعدوان أكثر من غيره وهو الذي يفوز في اللعبة ويعد من الناجحين.[12]

إن إعطاء المكافآت على استخدام العنف في تصميم الألعاب الإلكترونية وخياراتها المتنوعة تفتح أمام اللاعبين – ولاسيما صغار السن منهم، ومن يفضلون ألعاب المغامرة والعنف أكثر من غيرها – مجالات جديدة لتعلم ممارسة الحلول العنيفة والسلوك العدواني في النزاعات والمنافسات التي يمكن أن تُعرض حياة الشباب للخطر، وهي ممارسة تضع الأفكار العدوانية في المقدمة لأن الشاب على غرار الطفل يلعب ويتعلم في نفس الوقت، ويتجلى هذا الأمر بوضوح أكثر عندما يمارس هؤلاء اللاعبين حيلًا، وينفذون خططا لها علاقة بالعدوان.

وقد تستغل الجماعات الإرهابية هذه الألعاب وتسعى سعيًا حثيثًا لتجنيد أعضاء جدد وخاصة من الأطفال والشباب، ويمكن أن تلعب الألعاب الإلكترونية التي تمجد الشهادة دورًا مؤثرًا في جذب اهتمام انتحاريين في المستقبل وكذلك قد تستخدم المجموعات الإرهابية الألعاب الإلكترونية لأغراض تعليمية لبث الإرهاب الإلكتروني من خلال دعوة الأطفال والشباب إلى سرقة المنازل والأموال والمركبات وكذلك السطو على البنوك والتفجير والقتل [13].

فالعنف بمقتضى هذه الألعاب يتحول شيئًا فشيئًا إلى فعل وسلوك عدواني مألوف، يُلجأ له بديلًا عن أي نهج آخر، عندما يحين وقت النزاع وينفتح باب الصراع في واقع الحياة الاجتماعية. كما تعلم الأطفال والشباب أساليب ارتكاب الجريمة وفنونها وحيلها وتنمي لديهم القدرات العقلية ومهارات وأساليب العنف والعدوان التي تدفعهم لإرتكاب الأعمال الإرهابية بل يسعون ليكونوا جزء من المنظمات الإرهابية.[14]

الألعاب الإلكترونية أداة تجنيد لدى الجماعات الإرهابية

يستغل الإرهابيون الألعاب الإلكترونية المتصلة عبر شبكة الإنترنت على نطاق واسع لنشر الفكر المتطرف والمعتقدات الخاطئة والأفكار المغلوطة التي تسهل لديهم مهمة تجنيد أعضاء جدد في المنظمات الإرهابية سواءً كأعضاء أو كذئاب منفردة لتنفيذ عمليات انتحارية. وذلك من خلال نمذجة مقاطع الفيديو الخاصة بالمنظمات الإرهابية التي تسهم بالتجنيد الخاصة بهم وإدخالها في الألعاب الإلكترونية، وقد نجحت بل وتمكنت الجماعات الإرهابية من نشر دعاية واسعة النطاق وزيادة دعايتها من خلال وسائل سريعة وفعالة. فأصبحت هذه الظاهرة تهديداً عالمياً في السنوات الأخيرة حيث تمكن الإرهابيون من الوصول إلى عدد أكبر من الجماهير من خلال هذه الطرق والأساليب، والتي ساهمت في زيادة ملحوظة في تجنيد المزيد من الإرهابين في جميع أنحاء العالم ونمو كبير في عدد الهجمات الإرهابية وبالذات الهجمات التي يقوم بتنفيذها الذئاب المنفردة والخلايا النائمة.[15] وبسبب هذا الاتجاه، خصصت العديد

من الجماعات الإرهابية الكثير من مواردها وقدراتها لعالم الإنترنت وعلى وجه الخصوص الألعاب الإلكترونية، مما جعل من الصعب على الجهات الأمنية تتبع النشاط الإرهابي والحد من انتشاره. لذلك توصي العديد من الجهات الأمنية والمختصين والخبراء في المجال الأمني بالبقاء على اطلاع دائم بالمواد القانونية الخاصة بالأمن السيبراني للنظر في آثار الألعاب الإلكترونية العنيفة على اللاعبين عند صياغة السياسة العامة – مع تدابير مكافحة الإرهاب، للقبض على الإرهابيين بسهولة ومعرفتهم باستخدام التكنولوجيا الحديثة.

لقد فتحت شبكة الإنترنت فرصاً جديدة للإرهابيين للعمل في الخفاء دون رقابة أمنية عليهم، ونشر رسائلهم وأفكارهم المسمومة للفئات المستهدفة لديهم، وتحفيز وتدريب أتباعهم، وجمع الأموال، وكذلك تسهيل التخطيط لهجماتهم الإرهابية.[14] وأهم جانب يعتمدون عليه هو التفاعل الذي أدى إلى اتساع دائرة الاتصال عبر شبكة الإنترنت، مما زاد سهولة القضاء على الحدود الجغرافية الناجمة عن مسافة الموقع والعقبات الأمنية من جراء العبور عبرها، مما يسمح لهم بالاتصال الفوري مع بعضهم البعض في جميع أنحاء العالم دون رقابة أو حدود. وعلى الرغم من أن هذا التطور قد حفز النمو الاجتماعي والاقتصادي، إلا أن العديد من وسائل الإعلام والمنصات الاجتماعية – مثل فيسبوك – وغيرها من المنصات الإعلامية تستفيد أيضا من المحتوى الذي يداعب المشاعر ويحركها بالتعاطف مع المحتوى المنشور، مثل الصور التي تصور العنف أو المقاطع التي تظهر القتل وسفك الدماء. وتعمل المعلومات الحساسة نفسياً على تنشيط المشاعر المتباينة لدى الأشخاص، والتي تعمل على خلق مناقشات عالمية ومشاركة أكبر على وسائل التواصل الاجتماعي. يؤدي هذا إلى زيادة مشاهدات المنشور والتعليقات الموجودة تحته، مما يجعل النظام الأساسي الاجتماعي المعني أكثر قوة وشعبية، وستستمر هذه المنصة في كثير من الأحيان في تعزيز أو إهمال إزالة المحتوى لتحقيق مكاسب اقتصادية. بغض النظر عن الاهتمام، فإنه يميل إلى جذب، ما يجب أن يحدث بدلاً من التركيز على الحظر التام والفوري للمحتوى العنيف والمزعج.[16] هذه معضلة مقلقة يجب على الدول معالجتها أولاً من خلال التغييرات القانونية قبل السماح لمجتمع مكافحة الإرهاب بمعالجة الإرهاب والتطرف عبر الإنترنت.

بالإضافة إلى ذلك ساهمت جائحة كوفيد19- إلى دفع الكثير من الناس إلى قضاء المزيد من الوقت على الإنترنت من المنزل، مما زاد من خطر تعرضهم للمحتوى المتطرف والتطرف والتورط في العنف.[17] وقد منحت هذه الظروف الإرهابيين مجموعة كبيرة من الأهداف الضعيفة المعرضة لأساليب التطرف التي يستخدمونها. على وجه الخصوص، كان الناس يبحثون مؤخرا عن مواقع الترفيه والألعاب الإلكترونية كوسيلة للمشاركة في عالم افتراضي حيث يمكنهم التفاعل مع أشخاص من جميع أنحاء العالم وينتمون إلى مجتمع افتراضي. وبالتالي زيادة شعبية الألعاب وقدرتها على الوصول إلى جمهور كبير ومتنوع، وقد عملت العديد من المنظمات الإرهابية على جذب المزيد من المقاتلين والموالين لهم للعمل على أعدادهما للشروع في تنفيذ أعمال عنف دون أن تكون لها روابط جسدية بالنشاط الإرهابي.[18]

حيث تبث هذه المنصات ألعاب فيديو دولية عبر الإنترنت حيث يسمح للأفراد ببث الصوت والفيديو مباشرة لهم وهم يلعبون ألعاب الإلكترونية. على الرغم من أنه يهدف إلى مشاركة تجارب الألعاب مع الآخرين، إلا أن بعض الأفراد استخدموا غرف الدردشة لنشر معتقداتهم السياسية الاستقطابية والعنيفة حول القضايا المثيرة للجدل.

علاوة على ذلك، تم التحقيق في الألعاب الإلكترونية التي تطلق النار من منظور الشخص الأول ويجري التحقيق فيها حالياً لتأثيرها المحتمل في إزالة حساسية الأفراد تجاه العنف، وبشكل عام الترويج للعنف. أجرت جامعة نورث كارولينا في تشابل هيل في الولايات المتحدة دراسة اكتشفوا فيها أن الجماعات الإرهابية قد وجدت أنها تغير استراتيجيات التجنيد الخاصة بها بتسخير الألعاب الإلكترونية العنيفة من أجل جعل الانضمام إلى مجموعاتها أكثر جاذبية للمجندين المحتملين. وجد الباحثون المشاركون أن مقاطع فيديو الدعاية والتجنيد الخاصة بتنظيم داعش الإرهابي تنسخ ألعاب الكمبيوتر، وأبرزها Call of Duty. ألعاب First Person Shooter' (FPS) يلعبها مئات الملايين من الأشخاص، حيث لعبها أشخاص تحت سن 35 وبنسبة 90 % من الذكور، وهي هدف ديموغرافي رئيس للمنظمات الإرهابية. وتم اكتشاف أن مقاطع فيديو داعش غالباً ما تحاكي أو ترفع اللقطات وتقلد أنماط التحرير والميزات الشائعة والتسلسلات بطرق مفصلة قد يتعرف عليها اللاعبون العاديون فقط. وتتضمن هذه الألعاب لقطات تحفز على الإرهاب مثل «كيفية ظهور السلاح الذي يحمله مطلق النار في اللقطة، والتقدم من الأسلحة الأخف وصولاً إلى الأسلحة الثقيلة، واستخدام مقاطع لقطات الطائرات

بدون طيار، وطريقة استخدام الرسومات والعناوين».[19] لم يخلص الباحثون إلى أن ألعاب الإلكترونية مرتبطة ارتباطاً مباشراً بتطرف اللاعبين فقط، بل إن الجماعات الإرهابية مثل داعش قد صممت استراتيجيات التجنيد الخاصة بها لتكون مماثلة لتلك الموجودة في ألعاب Call of Duty و FPS من خلال إظهار وسائط إطلاق النار من منظور الشخص الأول في مقاطع الفيديو الخاصة بالتجنيد.[20] ومن المهم ملاحظة أن مصنعي الألعاب الإلكترونية لا يروجون لاستخدام العنف بل يسعون لتحقيق الأرباح. ومع ذلك، أصبحت المنظمات الإرهابية مثل داعش على دراية بشعبية ألعاب إطلاق النار من منظور الشخص الأول، وبالتالي قررت أنه باستخدام تقنيات ألعاب FPS، يمكنهم الوصول إلى جمهور أكبر عند محاولة تجنيد أعضاء جدد.

من المهم أن نلاحظ أن داعش معروف أيضا بتشجيع العنف ضد الأطفال الصغار باستخدام عدة طرق للترفيه المرتبط بالتكنولوجيا. على وجه التحديد Huroof وهو تطبيق تعليمي يطلب من الأطفال مطابقة الحروف العربية مع صور القنابل والأسلحة والدبابات والعديد من الرموز العسكرية الأخرى.[21] الأطفال ضعفاء ولكنهم سريعون في تعلم مواد جديدة، فمن المرجح أن تؤدي طريقة داعش في استهداف هذه الديموغرافية من خلال الترفيه إلى خلق جيل جديد من المقاتلين ذوي الإرادة القوية المخلصين لقضية داعش، دون أي اعتبار للقيم الأخلاقية أو الدمار الذي يخلفه العنف. ولا بد من معالجة هذا التنبؤ على المستوى الدولي، ويجب اتخاذ تدابير لضمان حصول هؤلاء الأطفال على التعليم الذي يحتاجون إليه بدلاً من تكتيكات إزالة المواد المنشرة من قبل الجماعات الإرهابية.

إن الجماعات الإرهابية مثل داعش ليست الجهات الفاعلة الوحيدة التي تزيد من تركيزها على الألعاب الإلكترونية وغيرها من المنصات عبر الإنترنت. فقد استلهمت المنظمات الإرهابية الأخرى والأقل تطوراً من إستراتيجيات التجنيد التي يتبعها داعش وبدأت في استخدام هذه التقنيات أيضا. قام فريق البحث في جامعة نورث كارولينا في تشابل هيل أيضا بتقييم العناصر الموجودة في تقنيات التوظيف المستوحاة من FPS ومقارنتها بناء على قيم إنتاجها. ووجدت الدراسة أن استراتيجية الألعاب الإلكترونية التي نوقشت سابقا «تم توسيعها لتغطي حوالي 50 نقطة تقييم تتراوح من قيم الإنتاج الفني إلى القصة وتقنية الكاميرا وحرفة التحرير وما إلى ذلك». باستخدام مقياس الدرجات هذا، حيث خلص الباحثون إلى أن فيديو داعش النموذجي تم إنتاجه على مستوى مماثل لفيديو الشركات المنتج بشكل احترافي.[22] إن استخدام هذه الأنواع من التقنيات للتجنيد يجعل من الواضح أن المنظمات الإرهابية أصبحت أكثر تعقيدا بشكل متزايد. إنهم يكيفون إستراتيجيات الاستقطاب الخاصة بهم مع مصالح الديموغرافية المستهدفة حتى يتمكنوا من تصميم حملات التجنيد الخاصة بهم لتكون جذابة لهم. المنظمات الإرهابية على استعداد لتعلم وممارسة واستخدام المهارات المختلفة التي قد لا يعتبرها الأفراد من خارج جماعتهم تهديداً. ومن المهم أيضا مراعاة أنه مع تزايد شعبية هذه التكتيكات، يمكن للمنظمات الإرهابية أن تتنافس فيما بينها لتحسين إستراتيجيات التجنيد الخاصة بها والوصول إلى عدد أكبر من المجندين المحتملين. إن جهودهم في ازدياد للتعرف على المجندين المحتملين وجذب أكبر عدد ممكن من الأتباع مما يدل على أن تهديد الإرهاب عبر الإنترنت سيستمر في الازدياد بشكل مكشوف والتكيف مع التفضيلات الشعبية التي لوحظت في هذا العصر الحديث.

وفي حين قد ينظر إلى أن استخدام تقنيات التجنيد من قبل المنظمات الإرهابية أمر سلبي، فإن زيادة انتشار تقنيات التجنيد بواسطة الألعاب الإلكترونية يمكن أن تساعد الأجهزة الأمنية في تحديد المنظمات الإرهابية. وقد ذكروا أن «دراسة مقاطع الفيديو الدعائية يمكن أن تساعد في تتبع انتشار طرق الإنتاج المتطورة وتطوير» بصمات جمالية «مفصلة يمكن استخدامها لتحديد الفرق والمنظمات التي تنتج مثل هذه المواد».[23] من خلال دراسة مقاطع الفيديو التي تنتجها المنظمات المتطرفة، يمكن لمسؤولي إنفاذ القانون والمسؤولين الحكوميين العمل معا لإدانة هذه الممارسات علنا وتحذير الأفراد على المستويين المحلي والدولي لرفع مستوى اليقظة عند التعامل مع أفراد مجهولين على منصات الإنترنت. إن فضح هذه التقنيات المتطورة عبر الأخبار والمصادر المطبوعة والكلام الشفهي يمكن أن يساعد الأفراد أيضا على فهم الأساليب التي يعتمد عليها الإرهابيون اليوم حتى يتمكنوا من تحديد النشاط الإرهابي والإبلاغ عنه إذا صادفوه. يجب على الوكالات والمنظمات والشركات أيضا زيادة التمويل لأقسام أو موظفي الأمن السيبراني من أجل تحسين تدابير الأمن السيبراني الحالية المصممة لمسح الإنترنت بحثاً عن اللغة أو الصور المتعلقة بالتطرف. كما من الأهمية أن يتعاونوا أيضا مع موظفي شركات التكنولوجيا الكبرى لضمان مشاركة هذه الشركات الكبيرة في هذه العملية، والتي قد تُحمل

كلاهما المسؤولية في الالتزام بجهودهم لحماية الجمهور من هذه الأساليب.

من الممكن ملاحظة نقطة تحول في مكافحة التطرف عبر الإنترنت، والتي تشهد حظر العديد من تطبيقات الدردشة الجماعية للمجتمعات المتطرفة والعنيفة من منصاتها. على سبيل المثال، قام Discord – وهو تطبيق دردشة جماعية شهير تم إنشاؤه في الأصل للاعبين – بإزالة المجموعات التي يتم تنظيمها حول العنف والأيديولوجيات المتطرفة.[24] هذا مهم لأنه يظهر أن المنصات الاجتماعية لديها القوة والسيطرة النهائية على كل ما يحدث داخلها. يعد تحديد المحتوى العنيف عملية معقدة، لكنها ممكنة. إن حظر جميع المجتمعات التي تحرض على العنف وتروج له يمكن أن يكون بمثابة رسالة تحذير إلى جميع أولئك الذين يعتزمون إنشاء جماعة متطرفة خاصة بهم.

تواصل مجموعة مكافحة الإرهاب مراقبة وتحليل المحتوى المتطرف والإرهابي المنشور على كل من المنصات الكبيرة والصغيرة على الإنترنت وتواصل إصدار تقارير تهدف إلى تحديد الجهات الفاعلة الرئيسة والتقنيات الجديدة التي يجب قراءتها. وتُبقي فريق مكافحة الجريمة على اطلاع دائم بأحدث التطورات في قوانين الخصوصية الألعاب الإلكترونية العنيفة، وتقوم برسم الروابط اللازمة الموجهة نحو التحليل لضمان عدم استغلال المنظمات المتطرفة للثغرات المحتملة أو انتهاك السياسة العامة. بالإضافة إلى ذلك، تمنح فرق الجريمة الأولوية لجمع المعلومات الاستخباراتية التي تشير إلى عمليات التطرف الإرهابي من المنصات الإعلامية المستخدمة على نطاق واسع مثل Twitch، والتي تبلغ حالياً عن حوالي 140 مليون زائر كل شهر.[25]

الأمن السيبراني:

يعتبر الأمن السيبراني تمامًا مثل قوات الأمن النظامية التي تسعى إلى حماية الممتلكات المادية والأشخاص من النشاط الإجرامي أو الإرهابي، فالأمن السيبراني يحمي أنظمة الكمبيوتر وتطبيقات المستخدم النهائي ومستخدمي تلك الأنظمة والبيانات التي يخزنونها.

فيهدف الأمن السيبراني إلى منع مجرمي الإنترنت أو القراصنة أو غيرهم من الوصول إلى أنظمة وتطبيقات تكنولوجيا المعلومات أو إلحاق الضرر بها أو تعطيلها أو تعديلها.

أهمية الأمن السيبراني

نظرًا لأن المجتمع البشري أصبح رقميًا، ودخلت جميع جوانب حياتنا من خلال شبكات الإنترنت وأجهزة الكمبيوتر والأجهزة الإلكترونية الأخرى وتطبيقات البرامج، حتى باتت جزء رئيس من البنية التحتية الحيوية، بما في ذلك الرعاية الصحية والمؤسسات المالية والحكومات والتصنيع، وأجهزة الكمبيوتر أو الأجهزة الذكية كجزء أساسي من عملياتها. وأصبحت كل هذه الخدمات والأجهزة والتطبيقات موصوله بشكل مستمر بشبكة الإنترنت.

يمتلك القراصنة الإلكترونيين حافزًا أكبر من أي وقت مضى لإيجاد طرق لاختراق أنظمة الكمبيوتر هذه، لتحقيق مكاسب مالية أو ابتزاز أو دوافع سياسية أو اجتماعية (**تُعرف باسم القرصنة**).

على مدى العقدين الماضيين، تم شن هجمات إلكترونية ضد البنية التحتية الحيوية في جميع الدول المتقدمة، وتكبد عدد لا يحصى من الشركات خسائر فادحة. هناك أكثر من 2000 انتهاك مؤكد للبيانات على مستوى العالم كل عام، مع كل خرق يكلف أكثر من 3.9 مليون دولار في المتوسط.[26] حيث يمكن أن تؤثر الانتهاكات والتهديدات الأمنية على أي نظام تقريبًا بما في ذلك:

الاتصالات – يمكن استخدام المكالمات الهاتفية ورسائل البريد الإلكتروني والرسائل النصية وتطبيقات المراسلة في الهجمات الإلكترونية.

الشؤون المالية – تعتبر المؤسسات المالية هدفًا أساسيًا للمهاجمين، وأي مؤسسة تعالج أو تتعامل مع معلومات البنك أو بطاقة الائتمان معرضة للخطر.

الحكومات – عادة ما يتم استهداف المؤسسات الحكومية من قبل قراصنة الإنترنت، الذين قد يحصلوا على معلومات المواطنين الخاصة أو البيانات العامة السرية.

النقل – السيارات المتصلة وأنظمة التحكم في حركة المرور والبنية التحتية للطرق الذكية كلها معرضة لخطر التهديدات السيبرانية.

الرعاية الصحية – أي شيء من السجلات الطبية في عيادة محلية إلى أنظمة الرعاية الحرجة في مستشفى وطني عرضة للهجوم.

التعليم – تتعرض المؤسسات التعليمية وبياناتها البحثية السرية والمعلومات التي بحوزتها عن الطلاب أو الموظفين لخطر الهجوم.

في الغالبية العظمى من هذه الأنظمة ، تعد مواقع الويب وتطبيقات الويب بوابة للمهاجمين. حيث إنهم معرضون

للإنترنت العام، ومتصلون بشكل عام بأنظمة خلفية حساسة، مما يمثل رابطًا ضعيفًا في إستراتيجية أمان المؤسسة.[27]

مبادئ الأمن السيبراني

الهدف الأساسي للأمن السيبراني هو حماية البيانات. يشير مجتمع الأمان عمومًا إلى مثلث من ثلاثة مبادئ ذات صلة تضمن أمان البيانات ، والمعروف باسم ثالوث وكالة المخابرات المركزية: [28]

السرية – ضمان إمكانية الوصول إلى البيانات الحساسة فقط لأولئك الأشخاص الذين يحتاجون إليها بالفعل، ويُسمح لهم بالوصول إليها وفقًا للسياسات التنظيمية، مع منع الوصول إلى الآخرين.

النزاهة – التأكد من عدم تعديل البيانات والأنظمة بسبب الإجراءات التي تتخذها الجهات المهددة، أو التعديل العرضي. يجب اتخاذ تدابير لمنع الفساد أو فقدان البيانات الحساسة، والتعافي بسرعة من مثل هذا الحدث في حالة حدوثه.

الاتصال المستمر – ضمان بقاء البيانات متاحة ومفيدة لمستخدميها النهائيين، وعدم إعاقة هذا الوصول بسبب عطل في النظام أو الهجمات الإلكترونية أو حتى الإجراءات الأمنية نفسها.

دور الأمن السيبراني في حماية صناعة الألعاب

تعد صناعة الألعاب من أكبر الصناعات الترفيهية في جميع أنحاء العالم، حيث بلغت قيمتها السوقية أكثر من 197 مليار دولار أمريكي في عام 2022م. وقد ساهمت جائحة كوفيد19- في زيادة هائلة في نموها بنسبة 26% في عامي 2019م و 2021م، حيث حاول المستخدمون ملئ وقتهم بعد فرض الإغلاقات، والتنبيه من عدم الاختلاط بين أفراد المجتمع لتكون الألعاب الملاذ الوحيد لهم. وتُعد هذه الصناعة المتنامية التي يتم تبادل الأموال والبيانات عبر الإنترنت هي عامل جذب للجهات الفاعلة [29].

يميل اللاعبون إلى الوثوق ببرامج الألعاب التي تحتوي على معلومات شخصية حساسة، مما يسمح لهم بإنفاق أموال حقيقية أو عملات مشفرة في مقابل الأشياء الثمينة داخل اللعبة، كلا النوعين من البيانات لهما قيمة ويجذب المتسللين لسرقتها. يمتلك المستخدمون القراصنة طرقًا مختلفة يستخدمونها بشكل شائع لاعتراض البيانات التي يمكن إعادة بيعها عبر الإنترنت أو لتحويل المعاملات إلى حساباتهم.

يحاول بعض القراصنة العثور على الثغرات الأمنية والاستفادة منها لتعطيل طريقة اللعب. قد تتسبب هذه الثغرات في حالات انقطاع الخدمة مما يضر باللعبة أو بسمعة الشركة، مما يكلفها مبالغ مالية عالية.

لذا من المهم التقيد ببروتوكولات الأمن السيبراني للوقاية من مخاطر تعطيل البيانات وسرقة العملات من المعاملات داخل اللعبة، ومنع الهجمات الإلكترونية على برامج الألعاب، والحد من إصابة الألعاب بالبرامج الضارة على أجهزة المستخدمين.

التهديدات السيبرانية التي تواجه صناعة الألعاب

تأتي التهديدات السيبرانية بأشكال مختلفة اعتمادًا على ما يحاول المتسلل تحقيقه وأين تكمن نقاط الضعف في برامج الألعاب. فهنا بعض التهديدات الإلكترونية الشائعة التي تؤثر على المستخدمين، فمنها الآتي:

1. تعديل اللعبة

تعديل اللعبة هو اختراق للعبة بدمج برامج غير نظامية في اللعبة نفسها. فإن هذا النوع من التهديد السيبراني هو الأكثر شيوعًا لعملاء الألعاب الصغيرة مثل الألعاب المحمولة. كما أنه شائع نسبيًا بالنسبة لألعاب الكمبيوتر التي تعمل بنظام Windows .

تتطلب هذه التعديلات معرفة متخصصة في الترميز ليتم إنشاؤها. عادةً لا تتطلب فقط معرفة لغة البرمجة ولكن تتطلب أيضًا معرفة في الترميز كون الكود المصدر الأولي غير متاح بشكل عام للاستخدام. تُباع التعديلات للمستخدمين من أجل الربح لمنحهم ميزة في اللعبة. خاصة في الألعاب متعددة اللاعبين عبر الإنترنت، حيث تؤثر هذه الإجراءات التي تتخذها التعديلات وتحبط المستخدمين الشرعيين الذين قد يغادرون اللعبة، تاركين اشتراكاتهم. لذا يجب على مطوري اللعبة إغلاق الثغرات التي يستخدمها القراصنة لإنشاء تعديلات. تضمن إزالة هذه الثغرات أن تستغرق التعديلات وقتًا طويلاً في البناء لتكون مربحة. [30]

2. تسرب معلومات الهوية الشخصية

تسريبات معلومات التعريف الشخصية هي نوع من الهجمات الإلكترونية حيث يتم جمع معلومات شخصية قيمة واستخدامها أو بيعها. حيث يمكن جمع البيانات بطرق مختلفة، بما في ذلك معالجة النماذج في لعبة ما

لجمع المعلومات الشخصية، أو مهاجمة مخازن البيانات التي تحتفظ بهذه المعلومات لمستخدمي اللعبة، أو الاستفادة من أخطاء المطورين التي تسبب بكشف بيانات المستخدمين. قد تتضمن البيانات التي تم جمعها رسائل البريد الإلكتروني وكلمات المرور ومعلومات بطاقة الائتمان ومعلومات الجهاز وغيرها من البيانات الشخصية والحساسة.

تعتبر ألعاب الهاتف المحمول عامل جذب خاص لتسريبات قواعد البيانات لأن الألعاب غالبًا ما تجمع البيانات تلقائيًا بدلاً من النماذج. تُقدّر الدراسات أن 14 ٪ من تطبيقات iOS و Android التي تستخدم التخزين السحابي معرضة للمشكلات التي تكشف عن معلومات تحديد الهوية الشخصية. في عام 2022 ، كشفت Neopets عن وجود اختراق للبيانات لمدة 18 شهرًا، مما أدى إلى الكشف عن المعلومات الشخصية لأكثر من 69 مليون مستخدم.[31]

3. هجمات التصيد

تحاول هجمات التصيد الاحتيالي الحصول على معلومات شخصية أو مدفوعات. سيرسل المهاجم رسالة متظاهرًا بفرد موثوق به أو خدمة تطلب معلومات شخصية. بمجرد جمع المعلومات، يمكن بيعها أو استخدامها في طلبات الفدية.

يعد التصيد الاحتيالي أحد أكثر الهجمات الإلكترونية انتشارًا على اللاعبين. على مدار عام واحد، اكتشف أحد حلول الأمان أكثر من 3.1 مليون إجراء تصيد في الألعاب عبر الإنترنت، وكان الهدف بشكل عام هو الحصول على بيانات اعتماد المستخدم لتولي حسابات الألعاب. تشمل الألعاب المستهدفة عناوين كبيرة، حيث تم إنشاء موقع ويب يقدم جيلًا من المكافآت داخل اللعبة لجمع بيانات الاعتماد.

غالبًا ما تتمتع حسابات الألعاب بإمكانية الوصول إلى معلومات الدفع التي يمكن سرقتها بعد ذلك، أو إذا كان اللاعب واحدًا من العديد ممن يعيدون استخدام كلمات المرور، فقد يتمكن المخترق من استخدام بيانات الاعتماد على مواقع أخرى لسرقة معلومات أكثر قيمة، بيانات الاعتماد هي طريقة هجوم إلكتروني حيث تُستخدم بيانات الاعتماد المسروقة لخرق أنظمة أخرى.[32]

4. هجمات DDoS

تهدف الهجمات الإلكترونية لرفض الخدمة الموزعة (DDoS) إلى إرباك حركة مرور الخادم العادية، مما يؤدي إلى إبطاء أو حظر الاتصالات المشروعة. يمكن ممارسة الضغط على هذه الهجمات ضد خوادم الألعاب، أو حظر الاتصالات للعديد من المستخدمين، أو استهداف الأجهزة الشخصية التي تعطل مستخدمًا واحدًا. يختلف الدافع وراء كل من هذه الهجمات الإلكترونية ويتطلب بيانات مختلفة.

تتسبب الهجمات على الأفراد بأن يصبح نظام ألعاب المستخدم عبر الإنترنت بطيئًا وغير قابل للتشغيل. يتم ذلك بشكل عام لاكتساب ميزة تنافسية على المستخدم المهاجم. يطلب المهاجم عنوان IP الخاص بالفرد، والذي يمكن الحصول عليه ببرامج ضارة. الهجمات الإلكترونية على منصات الألعاب عبر الإنترنت مثل PlayStation Network و Xbox Live تترك المستخدمين غير قادرين على لعب الألعاب المتصلة بالشبكة. ففي عام 2014م قامت مجموعة قراصنة بإغلاق شبكتي PlayStation & Xbox [33]

5. البرامج الضارة

تشكل بعض ألعاب الكمبيوتر والهاتف المحمول خطراً على أمان المستخدمين على الإنترنت والشخصي بسبب المتسللين أو أمان المطورين السيئ. قد تصاب الأجهزة ببرامج ضارة (فيروس) تهدف إلى سرقة البيانات بعد تنزيل ملف خاطئ أو برنامج مصاب بفيروس.

يمكن أن تصاب الألعاب التي تم تنزيلها ببرامج ضارة بعد أن يقوم أحد المتطفلين بحقن تعليمات برمجية ضارة في لعبة نظامية، أو يمكن للقراصنة إنشاء تطبيق مزيف يكون مجرد فيروس. هذا شائع بشكل خاص عند التنزيل من مواقع غير آمنة. تعد Minecraft واحدة من أكثر ألعاب الكمبيوتر المصابة بالبرامج الضارة بعد اكتشاف برامج ضارة على أكثر من 3 ملايين جهاز كمبيوتر بين عامي 2020 و 2021. [34]

حماية الألعاب من الهجمات الإلكترونية

تنجح الهجمات الإلكترونية عند حدوث إخفاقات في الأمن السيبراني في برامج الألعاب أو عندما يتم خداع المستخدمين لتقديم معلومات قيمة. يجب أن يفهم مطورو الألعاب أهمية تضمين الأمن السيبراني عند تطوير الألعاب وصيانتها لضمان الحفاظ على البيانات آمنة واستمرار اللعبة في العمل بشكل متوقع. يؤدي تضمين بروتوكولات الأمن السيبراني في جميع جوانب اللعبة ومراقبة بيانات اللعبة إلى تقليل مخاطر الهجمات الإلكترونية الناجحة.

بناء منظومة الأمن السيبراني في عملية تطوير اللعبة

يجب أن يكون الأمن أحد الأولويات التي تؤخذ في الاعتبار

عند تصميم وبناء البرامج. يجب أن تتضمن مراجعات الكود ومناقشات التصميم تحديد الثغرات الأمنية والمآثر المحتملة حتى يمكن إغلاقها قبل كتابة التعليمات البرمجية أو وضع التعليمات البرمجية في الإنتاج لتطبيق أفضل الممارسات لتطوير اللعبة ، مثل ممارسة نمذجة التهديد وتشغيل التحليلات الثابتة.

مراقبة الألعاب في الإنتاج

يجب جمع بيانات المراقبة ذات الصلة من البرنامج. ويمكن تصدير هذه البيانات إلى أداة مراقبة لرصد مشكلات الأمان. عندما يتوفر التنبيه الديناميكي والاستجابة التلقائية للحوادث ، يمكن للفرق الاستجابة للتهديدات الإلكترونية بسرعة ، مما يقلل من المستخدمين المتأثرين.[35]

طرق المصادقة الآمنة

يجب التأكد من أن أي كلمات مرور مخزنة محمية ومشفرة. بحيث تكون أساليب المصادقة آمنة باستخدام أساليب متعددة مثل المصادقة الثنائية للحماية من الهجمات الإلكترونية **كالآتي:**

بنية تحتية آمنة

تتضمن البنية التحتية في الألعاب قواعد البيانات والشبكات والخوادم (السحابية أو المحلية) التي تشغل التعليمات البرمجية. يجب أن تستخدم التعليمات البرمجية مبادئ أقل ثقة للحد من نطاق أي هجمات من خلال الخوادم. وضع الحماية على نقاط النهاية ضد هجمات DDoS ، حتى لا تتم مقاطعة تجربة اللعبة. و تأكد من أن قواعد البيانات مشفرة وآمنة، خاصة عند تخزين المعلومات الشخصية. حيثما أمكن ، افصل البيانات في مواقع تخزين مختلفة بحيث تكون الانتهاكات محدودة النطاق.

إجراء التمارين الأمنية

إجراء تمارين أمنية ضد لعبتك لتحديد جهات الهجوم المحتملة، يعد اختبار القلم والتكوين الجماعي الأحمر تمارين قيّمة للعثور على الثغرات الأمنية في الإنتاج وإغلاقها .

تثقيف المستخدمين

التفاعل مع المستخدمين حيثما أمكن ذلك. بحيث تقوم بتثقيفهم بشأن هجمات التصيد الاحتيالي والتأكد من وجود اتصالات واضحة حول البيانات التي قد تطلبها لعبتك منهم. وأبلغهم عندما يكون من المعروف أن محاولات التصيد الاحتيالي تحدث، بحيث تقل احتمالية اكتشافها. وحث المستخدمين على استخدام كلمات مرور قوية، وأبلغهم بتجنب إعادة استخدام كلمات المرور عبر التطبيقات المختلفة.[36]

المراجع

1. الشحروري، مها حسني(2008) : الألعاب الإلكترونية في عصر العولمة ما لها وما عليها ، القاهرة، دار الميسرة.26
2. الحمداني، شهباء جاسم(2011) : العنف في الألعاب الإلكترونية بالسلوك العدواني لدى تلاميذ المدارس الابتدائية، رسالة ماجستير، كلية التربية، جامعة تكريت ، العراق.
3. عبد الصادق، عادل (2015): الإرهاب الإلكتروني، نمط جديد وتحديات مختلفة، المركز العربي لأبحاث الفضاء الإلكتروني، السنة الرابعة عشرة– العدد 52، 92
4. عطية، أيسر محمد (2014): دور الآليات الحديثة للحد من الجرائم المستحدثة ، الإرهاب الإلكتروني وطرق مواجهته، الملتقى العلمي» الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من 2-4 /2014/9، عمان ، المملكة الأردنية الهاشمية.
5. Anderson, C. A., & Dill, K. E. (2000). Video games and aggressive thoughts, feelings, and behave-ior in the laboratory and in life. Journal of Personality and Social Psychology, 78.
6. Linder, J.F& Walsh, D.A.(2004), The Effects of Vident Video Game Hdoits on Adolescent Hostility, Aggressive Behaviors', and school performance, Tourmal of Adolescence, 27(1)
7. القليني، فاطمة يوسف (1995) : المخاطر الإعلامية الثقافية للطفل، دراسة الأبعاد السلبية لبعض الألعاب المستحدثة على الطفل المصري، المؤتمر السنوي الثالث(الطفل بين الخطر والإدمان)، القاهرة.
8. بقلاوة، داليا محمود(2009) : الألعاب التعليمية الإلكترونية ودورها في تنمية التفكير الإبداعي، مؤتمر التدريب الإلكتروني وتنمية الموارد البشرية، القاهرة، 12-13 أغسطس.

9. Anderson، C.A.، ed (2004) 'Violent Video GfOQies: Specific Effects of Violent Content on Aggressive Thoughts and Behaviour'، Advances in Experimental Social Psychology، 36
10. الصغيري، فريد(2013) :اللعبة الإلكترونية الممارسة الشبابية وعلاقتها بالعنف، مجلة دراسات وأبحاث ، جامعة الحليفة، الجزائر، ع 11.
11. Spink B، A.K .McPherson (2006) Quantifying the; Association Between Physical Activity and Injury in primary; School-Aged children، pediatrics، july1
12. خالد عبده الصرايره، 2008 النشر الإلكتروني وأثره على المكتبات ومراكز المعلومات عمان، كنوز المعرفة
13. بيتر غرايوسكي (2006) : جرائم الحاسب الآلي، الأبعاد العالمية في شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، مركز البحوث والدراسات الأمنية، 6-8 نوفمبر , 2006، الإمارات ،ط1.
14. «الشرق الأوسط – عودة تنظيم داعش في سوريا والعراق»، رؤى المخاطر العالمية، فبراير 2021،
https://globalriskinsights.com/202102//middle-east-the-resurgence-of-the-islamic-state-in-syria-and-iraq/
15. يونغ، إي «الإرهاب والإعلام وصعود الإنترنت» في ويذر، جي كي وموليتز، س. «مكافحة الإرهاب عبر الوطني»، بروكون، 2016
16. يونغ، إي «الإرهاب والإعلام وصعود الإنترنت» في ويذر، جي كي وموليتز، س. «مكافحة الإرهاب عبر الوطني»، بروكون، 2016
17. كوفيد19- والإرهاب في الغرب: هل انتشر التطرف حقا؟، Just Security، مارس 2021،
https://www.justsecurity.org/75064/covid-19-and-terrorism-in-the-west-has-radicalization-really-gone-viral/
18. «تطرف جومانجي؟ كيف يمكن للألعاب والتلعيب تسهيل عمليات التطرف»، مجلة نزع التطرف، 2020،
https://journals.sfu.ca/jd/index.php/jd/article/view/359223/
19. Twitch Streamer Destiny يفقد الشراكة بسبب «تشجيع العنف»، Ginx، سبتمبر 2020،
https://www.ginx.tv/en/twitch/twitch-streamer-destiny-loses-partnership-for-encouraging-violance-against-protesters
20. كيف يتحول «نداء الواجب» إلى دعوة للجهاد، الأمن الداخلي اليوم، أغسطس 2019،
https://www.hstoday.us/subject-matter-areas/counterterrorism/how-call-of-duty-is-transformed-into-a-call-for-jihad/
21. تطرف جومانجي؟ كيف يمكن للألعاب والتلعيب تسهيل عمليات التطرف»، مجلة نزع التطرف، 2020،
https://journals.sfu.ca/jd/index.php/jd/article/view/359223/
22. كيف يتحول «نداء الواجب» إلى دعوة للإرهاب الأمن الداخلي اليوم، أغسطس 2019،
https://www.hstoday.us/subject-matter-areas/counterterrorism/how-call-of-duty-is-transformed-into-a-call-for-jihad/
23. كيف يتحول «نداء الواجب» إلى دعوة للإرهاب، الأمن الداخلي اليوم، أغسطس 2019،
https://www.hstoday.us/subject-matter-areas/counterterrorism/how-call-of-duty-is-transformed-into-a-call-for-jihad/
24. «تطبيق الدردشة الجماعية Discord يقول إنه حظر أكثر من 2 مجتمع متطرف»، NPR، أبريل 000،
https://www.npr.org/202105/04/2021//group-chat-app-discord-says-it-banned-more-than-9838557532--extremist-communities?t=000
25. «إحصائيات استخدام ونمو Twitch: كم عدد الأشخاص الذين يستخدمون Twitch في عام 2021؟»، BackLinko، يناير 2021،
https://backlinko.com/twitch-users
26. What is Ethical (White Hat) Hacking | CEH Certification | Imperva
27. https://coralogix.com/blog/gaming-need-cyber-security/#:~:text=Cybersecurity%20protocols%20are%20necessary%20to,malware%20infections%20on%20users'%20devices.
28. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-principles#:~:text=These%20cyber%20security%20principles%20are,to%20identify%20cyber%20security%20incidents.
29. بقيمة 175 مليار دولار ونمو 19% خلال 2020.. الألعاب الإلكترونية.. أرباح بالملايين للشركات واللاعبين - بوابة الأهرام (ahram.org.eg)
30. https://www.videogameschronicle.com/news/destiny-2-cheat-creator-agrees-to-pay-bungie-135--million-in-damages/
31. https://www.zimperium.com/blog/unsecured-cloud-configurations-exposing-information-in-thousands-of-mobile-apps/
32. https://securelist.com/gaming-related-cyberthreats-2021107346/2022-/#:~:text=One%20of%20the%20most%20widespread,account%20credentials%20or%20financial%20information.
33. https://coralogix.com/blog/ddos-attack-political-cyber-attack/
34. https://vpnoverview.com/internet-safety/malware/malware-infected-games/
35. https://coralogix.com/blog/observability-security-work-together/
36. https://coralogix.com/blog/red-teaming-cybersecurity/