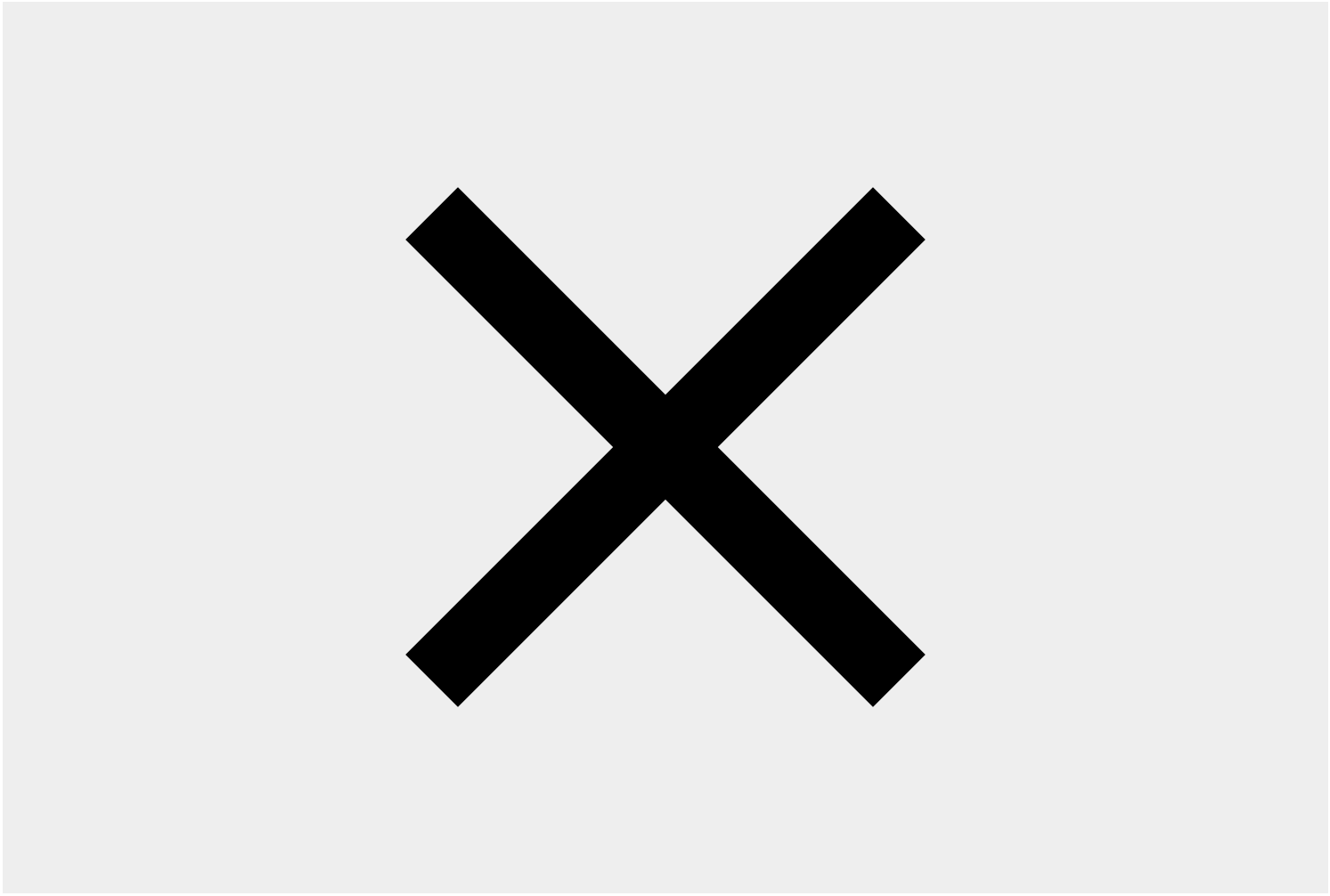
الأمن السيبراني

Posted on 2021 ,10 نوفمبر



Category: التحول الرقمي

بواسطة :

وقد قمت بإعادة صياغة التعريف ليكون PwC **الأمن السيبراني** ، للأمن السيبراني تعريفات متعددة، لكن أشملها هو تعريف شركة :أكثر شمولاً ووضوحا

يُقصَد بالأمن السيبراني هو تلك التكنولوجيا والعمليات والضوابط الهادفة إلى حماية الأنظمة والبرامج والشبكات، من خطر الهجمات الرقمية التي تحاول الوصول إلى البيانات المهمة أوالمعلومات الحساسة تغييراً أو إتلافاً للبيانات والمعلومات، أو تعطيلاً .للخدمات

استثمارات الأمن السيبراني

بلغ الاستثمار عالمياً في الأمن السيبراني عام 2019 حوالي 49 مليار دولار، وارتفع إلى 54 مليار دولار عام 2021، وكان لجائحة كورونا الدور الأبرز في زيادة هذه الاستثمارات على الأمن السيبراني نظراً للاعتماد الكبير على أدوات التحول الرقمي خلال هذه .www.statista.com الجائحة. هذه البيانات وفقاً لتقرير حديث صدر في مارس 2021 في الموقع

فرص الأمن السيبراني

باب الفرص للأمن السيبراني مفتوح على مصراعيه خصوصاً مع تزايد الاعتماد على أدوات التحول الرقمي. ففي الوقت الذي بلغ فيه حجم السوق للأمن السيبراني حوالي 100 مليار دولار عام 2017، فإنه من المتوقع أن يرتفع هذا الرقم بشكل أكبر ليصل حجم في www.statista.com سوق الأمن السيبراني إلى حوالي 175 مليار دولار عام 2024 وفقاً لأحدث تقرير نشره الموقع السابق هذا الشهر يوليو 2021

إن هذا الحجم الكبير لسوق أمن المعلومات، يفتح الفرص العديدة والواعدة أمام المتخصصين في أمن المعلومات حيث تصل المسميات الوظيفية في هذا المجال إلى أكثر من عشرين مسمى وظيفي، والسوق في أمس الحاجة إلى مثل هذه التخصصات في .أمن المعلومات

تحديات الأمن السيبراني

هناك تحديات كبيرة تقف في طريق الأمن السيبراني، وتزداد هذه التحديات كلما ازداد الاعتماد على تكنولوجيا المعلومات، وأدوات التحول الرقمي. هذه التحديات تتعدد صورها، وتتغير أشكالها، وتتفرع وسائلها، فتظهر بطرق مختلفة، يتفاوت ضررها، ويتباين :خطرها، وهذه قائمة بأبرز سبع تحديات أو تهديدات للأمن السيبراني

- .هجمات المصيَدة
- .هجمات الثغرات الأمنية في التطبيقات والبرامج وأنظمة التشغيل
- .هجمات إنترنت الأشياء
- .هجمات الحوسبة السحابية
- .هجمات الأجهزة القديمة الخارجة عن الدعم الفني
- .هجمات الفيروسات
- .هجمات الذكاء الاصطناعي

وللمعلومة

فالحرب ضروس، حامية الوطيس، والنزال سجال بين الطرفين: بين من يطورون الأدوات المهاجِمة، ومن يطورون الأنظمة لصدها، ويصممون التطبيقات لمواجهتها. ولكل تحدٍ من التحديات المذكورة آنفاً حلول يجب الأخذ بها، والحرص عليها، والمتابعة لها، لنكون ـ أفراداً وشركاتٍ وحكوماتٍ ـ في مأمن من أضرار الحروب السيبرانية، والهجمات الإلكترونية، والجرائم .الرقمية

تطبيقات الأمن السيبراني

للأمن السيبراني العديد من التطبيقات التي تتفاوت في قدراتها الدفاعية، وإمكاناتها الأمنية في التصدي للهجمات الإلكترونية، ومواجهة الجرائم الرقمية. والقائمة لهذه التطبيقات تطول، ولكن يمكن حصرها في ستة تطبيقات، تعتبر هي التطبيقات المصنَّفة كقائدة لتطبيقات الأمن السيبراني وفقاً لأحدث تقرير نشرته جارتنر في مايو 2021، وهو تقرير سنوي يصدر عن هذه الشركة المعتبرة عالمياً، حيث أخضعت 19 تطبيقاً ونظاماً متخصصاً في الأمن السيبراني بناء على قواعد صارمة ومعايير حازمة، وكانت :النتيجة أن ستة أنظمة منها فقط، تم تصنيفها كتطبيقات قائدة للأمن السيبراني، وإليكم قائمة هذه التطبيقات

- Microsoft Defender ميكروسوفت ديفيندر
- CrowdStrike كراودستريك
- TrendMicro ترند ميكرو
- SentinelOne سينتاينيل ون
- McAfee مكافي
- Sophos سوفوس

عوائد الأمن السيبراني

مليار دولار هو إجمالي العوائد التي جنتها الشركات المقدمة لحلول أمن المعلومات على مستوى العالم بحسب تقرير نشره 4.2 في سبتمبر 2020 www.statista.com موقع

في يونيو 2020، حيث أوضح هذا التقرير أن متوسط العائد على www.smart-energy.com كما أشار تقرير آخر نشره موقع الاستثمار في الأمن السيبراني يصل إلى 179% وفقاً لدراسة استقصائية شملت أكثر من 1000 شركة تعمل في 13 صناعة في 19 .دولة

الدراسة بينت أن هذه الشركات أنفقت حوالي 10 مليون دولار على الأمن السيبراني عام 2019، وتوزع هذا الاستثمار على ثلاث :مساحات

- .%العنصر البشري، والعائد على الاستثمار فيه وصل إلى 252
- .%العمليات، والعائد على الاستثمار فيها وصل إلى 156

.%التكنولوجيا، والعائد وصل إلى 129 •

تأثيرات الأمن السيبراني

للأمن السيبراني تأثيراته السلبية في حال لم يتم عمل المطلوب حيال التهديدات الإلكترونية، ولم يؤخذ في الاعتبار ارتفاع الهجمات .الرقمية مع تزايد الاعتماد على أدوات التحول الرقمي

وللتخفيف من خطر ذلك، فإنه يوصى بأخذ الاحتياطات الأمنية، على مستوى الأفراد والشركات والمؤسسات، ومن ذلك على سبيل :المثال

على مستوى الأفراد •

عمل التحديثات الجديدة للتطبيقات على كافة الأجهزة الإلكترونية سواء كانت جوالات أو كمبيوترات أو غيرها، وذلك من المواقع الموثوقة لمطوري هذه الأنظمة والتطبيقات

عدم الدخول على الروابط غير الموثوقة التي تصل عبر البريد الإلكتروني أو الرسائل القصيرة أو وسائل التواصل الاجتماعي

استخدام طريقة تعدُّد المصادقة للدخول على الحسابات المختلفة للفرد، فإن ذلك يقلل من خطورة الاختراق، فحتى لو تم معرفة كلمة السر، فإن طريقة تعدد المصادقة، تطلب طريقة أخرى للدخول على الحساب مثل إدخال الشفرة المرسلة عبر جهاز الجوال، .أو عمل مصادقة ثنائية عبر تطبيق المصادقة

على مستوى الشركات والحكومات •

.ضرورة الاستثمار في أنظمة وتطبيقات أمن المعلومات، واستخدام الأفضل والأقوى منها

ضرورة وجود فريق متخصص في أمن المعلومات، من مهامه تنفيذ تطبيق أفضل الممارسات في أمن المعلومات، وتوعية الأفراد، ورفع حسهم الأمني لمواجهة تهديدات الهجمات الإلكترونية، وصد الجرائم الرقمية، حفاظاً على أصولهم المعلوماتية أو بياناتهم .الشخصية من الاختراق أو الإتلاف أو الابتزاز

الخلاصة

لقد ذكرتُ في بداية هذا المقال أن الأمن السيبراني هو الحارس الأمين، والحامي المكين لبقية أدوات التحول الرقمي، والحقيقة أنه كذلك. فمع تبادل البيانات الضخمة من المصادر المتعددة سواء كانت إنترنت الأشياء، أو تحليل البيانات، تزداد الهجمات الرقمية، والجرائمة الإلكترونية مستهدفة الأفراد والشركات والحكومات بغية الوصول إلى بياناتهم، واستخدامها لمصلحة الجهات المهاجِمة .أو الكيانات المخترِقة، بغرض الابتزاز أو التجسس أو التعطيل والتخريب

لذلك يشكِّل الأمن السيبراني أحد مصادر القلق، ومواطن الخوف، ومكامن الرعب بالنسبة للأفراد والشركات والحكومات على .السواء

وقد صنف منتدى الاقتصاد العالمي الهجمات الإلكترونية ضمن أكبر خمسة مخاطر عالمية تهدد المجتمع الدولي عام 2019، وبعد جائحة كورونا حيث ازدادت وتيرة هذه الهجمات، ارتفع تصنيف خطرها إلى المرتبة الأولى في تقرير منتدى الاقتصاد العالمي عام 2020

وفي نهاية النهاية لهذا المقال، جدير بالذكر أن هناك تداخلاً وتفاعلاً بين تقنية الأمن السيبراني والذكاء الاصطناعي، حيث يستخدم المطورون تكنولوجيا الذكاء الاصطناعي لصقل قدرات تطبيقات الأمن السيبراني، فقد أصبحت هذه التطبيقات تتعلم ذاتياً، وتطور من إمكاناتها آليا للتصدي للهجمات الإلكترونية، ومواجهة الجرائم الرقمية دون تدخل العناصر البشرية.