



الانباء
الراعي الإعلامي الحصري للمنتدى

ملتقى الحكومة الإلكترونية الثالث

برعاية سمو رئيس الوزراء وتنظيم «نوف إكسبو»
15 - 17 نوفمبر



3 أسباب وراء استهداف منطقة الشرق الأوسط من المهاجمين للمواقع الإلكترونية

الجلسة الثانية



(قاسم باشا)

من اليمين مروان خلف واسامة عبدو وسعود الصبيح ونزار وفا وراي كافييتي

أساليب الهجوم على مواقع المؤسسات باستخدام برامج مثل APT وATA. وأوضح عبدو أن هناك منشآت تخترق شبكاتها دون أن تعلم وهي بذلك تتعرض لأضرار وخيمة سواء مالي أو معلوماتي، لافتاً إلى أن هناك حالات اختراق تبدأ من يوم واحد وتستغرق حتى عامين، وهو ما يعرض المنشأة لخطر الاختراق لاستنزاف على مستوى البيانات والخطط الاستراتيجية.

وأشار وفا إلى أن المخاطر ناتجة عن أن 90٪ من الموظفين العاملين بالمؤسسة أو المنشأة يستخدمون مواقع التواصل الاجتماعي على ذات الأجهزة المستخدمة في إدارة أعمال المؤسسة، كما أنه يتم تحميل الكثير من التطبيقات على ذات الأجهزة المستخدمة في إدارة الأعمال، وهو ما يسمح للمهاجمين باختراق هذه الأجهزة.

وأفاد بان نحو 78٪ من المؤسسات التي اخترقت مواقعها الإلكترونية من قبل مهاجمين كانت بسبب الإهمال وسلوكيات خاطئة من قبل الموظفين العاملين بها. أما مهندس النظم في شركة Fortinet أسامة عبدو فقال إن التهديدات تتزايد بشكل كبير خاصة مع قيام المهاجمين بتطوير

اقتصاديّة سوداء، لافتاً إلى أن السعودية تتعرض لهجمات بنسبة 11٪، وأن كلا من ألمانيا وإسبانيا تتعرض لهجمات بنسبة 10٪. ضرورة قيام المؤسسات المستهدفة من قبل المهاجمين السيرانيين بتطوير وسائل الحماية ضد تلك التهديدات من خلال وضع نظم وأطر حماية تتمتع بالرونة اللازمة.

من جهته، قال مدير تطوير الخدمات الأمنية في شركة Cisco المهندس نزار وفا إن عمليات اختراق موقع ما يحتاج أحياناً لإيام لاكتشاف أنه تم اختراقه، لذا يجب العمل على إيجاد آلية أو أطر تعمل على سرعة كشف هذه الاختراقات.

وأشار وفا إلى أن نحو 90٪ من المخاطر ناتجة عن أن الموظفين العاملين بالمؤسسة أو المنشأة يستخدمون مواقع التواصل الاجتماعي على ذات الأجهزة المستخدمة في إدارة أعمال المؤسسة، كما أنه يتم تحميل الكثير من التطبيقات على ذات الأجهزة المستخدمة في إدارة الأعمال، وهو ما يسمح للمهاجمين باختراق هذه الأجهزة.

وأفاد بان نحو 78٪ من المؤسسات التي اخترقت مواقعها الإلكترونية من قبل مهاجمين كانت بسبب الإهمال وسلوكيات خاطئة من قبل الموظفين العاملين بها. أما مهندس النظم في شركة Fortinet أسامة عبدو فقال إن التهديدات تتزايد بشكل كبير خاصة مع قيام المهاجمين بتطوير

اقتصاديّة سوداء، لافتاً إلى أن السعودية تتعرض لهجمات بنسبة 11٪، وأن كلا من ألمانيا وإسبانيا تتعرض لهجمات بنسبة 10٪. ضرورة قيام المؤسسات المستهدفة من قبل المهاجمين السيرانيين بتطوير وسائل الحماية ضد تلك التهديدات من خلال وضع نظم وأطر حماية تتمتع بالرونة اللازمة.

من جهته، قال مدير تطوير الخدمات الأمنية في شركة Cisco المهندس نزار وفا إن عمليات اختراق موقع ما يحتاج أحياناً لإيام لاكتشاف أنه تم اختراقه، لذا يجب العمل على إيجاد آلية أو أطر تعمل على سرعة كشف هذه الاختراقات.

وأشار وفا إلى أن نحو 90٪ من المخاطر ناتجة عن أن الموظفين العاملين بالمؤسسة أو المنشأة يستخدمون مواقع التواصل الاجتماعي على ذات الأجهزة المستخدمة في إدارة أعمال المؤسسة، كما أنه يتم تحميل الكثير من التطبيقات على ذات الأجهزة المستخدمة في إدارة الأعمال، وهو ما يسمح للمهاجمين باختراق هذه الأجهزة.

وأفاد بان نحو 78٪ من المؤسسات التي اخترقت مواقعها الإلكترونية من قبل مهاجمين كانت بسبب الإهمال وسلوكيات خاطئة من قبل الموظفين العاملين بها. أما مهندس النظم في شركة Fortinet أسامة عبدو فقال إن التهديدات تتزايد بشكل كبير خاصة مع قيام المهاجمين بتطوير

اقتصاديّة سوداء، لافتاً إلى أن السعودية تتعرض لهجمات بنسبة 11٪، وأن كلا من ألمانيا وإسبانيا تتعرض لهجمات بنسبة 10٪. ضرورة قيام المؤسسات المستهدفة من قبل المهاجمين السيرانيين بتطوير وسائل الحماية ضد تلك التهديدات من خلال وضع نظم وأطر حماية تتمتع بالرونة اللازمة.

من جهته، قال مدير تطوير الخدمات الأمنية في شركة Cisco المهندس نزار وفا إن عمليات اختراق موقع ما يحتاج أحياناً لإيام لاكتشاف أنه تم اختراقه، لذا يجب العمل على إيجاد آلية أو أطر تعمل على سرعة كشف هذه الاختراقات.

وأشار وفا إلى أن نحو 90٪ من المخاطر ناتجة عن أن الموظفين العاملين بالمؤسسة أو المنشأة يستخدمون مواقع التواصل الاجتماعي على ذات الأجهزة المستخدمة في إدارة أعمال المؤسسة، كما أنه يتم تحميل الكثير من التطبيقات على ذات الأجهزة المستخدمة في إدارة الأعمال، وهو ما يسمح للمهاجمين باختراق هذه الأجهزة.

كافييتي: المنشآت

النضوية والبنوت

أكثر المؤسسات

المستهدفة من

المهاجمين

وفا: 90٪ من

المخاطر سببها دخول

الموظفين لمواقع

التواصل الاجتماعي

عبر أجهزة العمل

عبدو: منشآت

تخترق شبكاتنا دون

أن تعلم وتعرض

لأضرار وخيمة مالياً

ومعلوماتياً

خلف: تنامي الطلب

على الخدمات

الإلكترونية مع

التوسع في استخدام

الهواتف الذكية

شريف حمدي

تطرق الجلسة الثانية

لمسار أمن المعلومات

والمخاطر الأمنية الموجهة

داعياً إلى هذا الصدد إلى

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

التخطيط الاستراتيجي

وإدارة المخاطر مدير إدارة

الحكومات الناجحة تصل بخدماتها إلى الناس ولا تنتظر قدومهم

الجلسة الأولى



(قاسم باشا)

من اليمين جوزيف خوري وباتريسيا فلوريبي وليالي المنصوري وبول لانج وويلم كلابارت

طارئ قد يحدث من حوادث أو جرائم، مشيراً إلى أن الحكومة مطالبة بالاستماع إلى مواطنيها من خلال وسائل التواصل الاجتماعي وذلك بالتفاعل مع طالبات مواطنيها واستقاء آرائهم حول خدماتها المختلفة وقياس مستوى هذه الخدمات ومن ثمة تحديد البرامج لتبنيها.

وأشار إلى أن الحكومات تنتقل إلى الخدمات المتنقلة والمواطن أصبحوا متطلبين جداً مثل «جيمس بوند»، لذلك عليها أن تتصرف بموجب متطلباتهم.

إدارة العلاقات

ومن جانبه، استعرض جوزيف خوري من ميكروسوفت حلول إدارة العلاقات مع العملاء للحكومة الديناميكية، مشيراً إلى أنه يوجد نوع من التفاعل بين المواطن والجهات الحكومية عبر تطبيقات مختلفة يمكن أن تتجمع في منصة واحدة لتسهيل عمل الجهات الحكومية المختلفة. وأكد أن المنصة الواحدة التي تحتوي على أكثر من تطبيق لمختلف الجهات الحكومية تمكن من الاستجابة للمراسلة بين الجهات وقياس رضا العملاء وخدمة العديد من الطلبات، مشيراً إلى أن شركة ميكروسوفت تمتلك منصات تستطيع أن تخدم 20 تطبيقاً من خلال منصة واحدة، وهذا من شأنه أن يقلل الكلفة على الحكومات.

وقال خوري إن المواطن ليس بحاجة إلى الانتقال إلى مقر جهة حكومية لتقديم شكواه بل يمكنه عن طريق قنوات

في المؤسسة التي تعرضت لعملية الاختراق وكشف تفاصيل العملية من حيث متى تمت عملية الاختراق وإلى أي مدى وصلت، فضلاً عن تتبع من قاموا بهذا العمل.

ولفت إلى أن المهاجمين يحدون قبل القيام بالهجوم على المؤسسة المستهدفة مواطن الضعف في برامج الحماية ويعرفون كيف يتغلبون عليها، مشيراً إلى أن نحو 69٪ من العملاء

يعرفون أنهم مخترقون من جهات خارجية وهو ما يكشف ضعف نظم الحالية لديهم.

وذكر أن شركة Fire Eye تعمل منذ 2004 على اكتشاف التهديدات وتحليل هذه التهديدات لمنعها قبل وقوعها، لافتاً إلى وجود مجموعات معينة من المهاجمين يختصون في استهداف أنواع معينة من العملاء سواء مؤسسات حكومية لأهداف استخباراتية

معرفة أهدافها وسائل التواصل الاجتماعي وغيرها من الوسائل الحكومية عن طريق اللوحات الإلكترونية الذكية أو الهواتف الذكية.

معايير جديدة من جهتها، كشفت باتريسيا فلوريبي من شركة إيماك حول «مدن المستقبل الآن» أن المدن الذكية تضمن المشاركة الشعبية الفعالة وتوفير الخدمات الحكومية على نطاق واسع وفي كل مجالات الحياة. ودعت الحكومات إلى ضرورة إعداد معايير جديدة للمحتوى الإلكتروني الذي يتوافق مع التقنيات المتطورة التي يتم تطبيقها بجهود حثيئة تدعم خيارات التطوير المتبعة في المدن والبلديات وإعداد نماذج رائدة في المنطقة كنماذج عبر تطبيقات مختلفة يمكن أن تتجمع في منصة واحدة لتسهيل عمل الجهات الحكومية المختلفة. وأكد أن المنصة الواحدة التي تحتوي على أكثر من تطبيق لمختلف الجهات الحكومية تمكن من الاستجابة للمراسلة بين الجهات وقياس رضا العملاء وخدمة العديد من الطلبات، مشيراً إلى أن شركة ميكروسوفت تمتلك منصات تستطيع أن تخدم 20 تطبيقاً من خلال منصة واحدة، وهذا من شأنه أن يقلل الكلفة على الحكومات.

وقال خوري إن المواطن ليس بحاجة إلى الانتقال إلى مقر جهة حكومية لتقديم شكواه بل يمكنه عن طريق قنوات

في المؤسسة التي تعرضت لعملية الاختراق وكشف تفاصيل العملية من حيث متى تمت عملية الاختراق وإلى أي مدى وصلت، فضلاً عن تتبع من قاموا بهذا العمل.

ضرورة تطوير

الحكومات لخدماتها

الذكية وتبني

المشاريع لتفعيل

ربط الأفراد مع

منصات مبتكرة

75٪ من المواطنين

سيستعملون مع

الحكومة عن طريق

الهواتف الذكية

بنهاية 2015

وفي البداية، أكد ويلم كلابارت من شركة «أي بي. بي.» على أهمية التطبيقات التي تحتاجها الحكومة في الحفاظ على سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

مخاطر من شأنه أن يهدد سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

مخاطر من شأنه أن يهدد سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

مخاطر من شأنه أن يهدد سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

مخاطر من شأنه أن يهدد سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

مخاطر من شأنه أن يهدد سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

مخاطر من شأنه أن يهدد سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

مخاطر من شأنه أن يهدد سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

مخاطر من شأنه أن يهدد سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

مخاطر من شأنه أن يهدد سلامة المواطنين والنظام العام في الطرقات وتنظيم حركة المرور والاستجابة لأي

الجلسة الثالثة

69٪ من العملاء يعرفون أنهم مخترقون من جهات خارجية

وهي: ● تعظيم برامج الأمن المعلوماتي. ● العمل على وضع الحلول والتقنيات لوقف التهديدات المتقدمة والمستمرة.

● العمل على حماية البيانات وليس حماية المكان فقط. أما مهندس النظم في شركة Fortinet أسامة عبدو فقال: إن مخاطر أمن المعلومات تزداد بشكل لافت في ظل تطور نظم اختراق مواقع الهيئات الحكومية والقطاع الخاص.

ولفت إلى أن المستقبل سيشهد طرح برامج إضافية للبرامج الحالية التي تساعد في كشف المهاجمين الذين يستخدمون برامج مشابهة، مبيناً أن الإيميلات من أكثر الوسائل المستخدمة في عمليات الهجوم كونها تحمل فيروسات تساعد هؤلاء في عمليات الاختراق.

وأوضح عبدو أن المؤسسات تحتاج إلى شبكات مؤمنة بنظم الحماية المتكاملة والمتقدمة. من جهته، تحدث مدير إدارة تطوير النظم بشركة «كي نت»، عن دور الشركة في تطوير خدمات الدفع الإلكتروني في القطاع

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

وأيضا لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

وأيضا لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

وأيضا لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

وأيضا لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

وأيضا لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية



(أحمد علي)

من اليمين خالد بوعباس وعمر البرغوثي وليالي المنصوري واسامة عبدو

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

تكون أيضاً لأهداف تدمير بعض المنشآت إما لأغراض المنافسة أو لأغراض سياسية. وقال البرغوثي إن نظم التهديدات تتغير تماماً مثل الموضة وتشهد تطور مستمر بهدف تخطي نظم الحماية، مضيفاً أننا نعيش في حرب معلوماتية مستمرة ومنظمة، لذا يجب التفكير دائماً في دعم مؤسساتنا. وأكد أهمية توافر 3 أمور عند الحديث عن الحماية

القطار: يمكن

تحديد متى بدأت

عملية الاختراق

وإلى أي مدى

وصلت

البرغوثي: يجب

تعظيم برامج

الأمن المعلوماتي

والعمل على وقف

التهديدات

بوعباس: 1,4

مليون عملية دفع

تتم يومياً عبر شبكة

«كي نت»

شريف حمدي

شهدت الجلسة الثالثة من منتدى الحكومة الإلكترونية الثالث والتي حملت عنوان «أمن المعلومات مسار متعدد الجوانب» برئاسة م. ليالي المنصوري من الجهاز المركزي لتكنولوجيا المعلومات نقاشاً حول مخاطر أمن المعلومات.

وقال المتخصص في المنتجات الاستراتيجية في شركة Fire Eye إباد القطارة إن الشركة تعمل في مجال كشف التهديدات المتقدمة منذ 10 سنوات، مؤكداً في هذا السياق أن خريطة المهاجمين لشبكات ومواقع الجهات الحكومية والقطاع الخاص تتطور بشكل مستمر وبطريقة ممنهجة.

وأوضح أن عمليات الاختراق تتم في كثير من الأحيان خاصة عند مهاجمة المؤسسات الحيوية بشكل تدريجي حتى الوصول إلى أن المهاجم يمكنه استخدام الشبكة مثل أي مستخدم داخل المؤسسة وهو أمر خطير.

وأفاد القطارة بأن الشركة لديها نظم متطورة يمكنها من خلالها إجراء التحقيق

في المؤسسة التي تعرضت لعملية الاختراق وكشف تفاصيل العملية من حيث متى تمت عملية الاختراق وإلى أي مدى وصلت، فضلاً عن تتبع من قاموا بهذا العمل.