قرصنة المعلومات

قرصنة المعلومات تعني استخدام منظومة المعلومات عن غير وجه حق. هي جريمة خطيرة. استيلاء المُجرمين على البيانات الشخصية من الممكن أن يُثير قلقًا كبيرًا. لقد جمعنا على هذه الصفحات معلومات عن قرصنة المعلومات بشكل عام وكذلك نقدم المشورة بشأن كيفية التعامل إذا كنت تشك بأنك قد تعرضت لقرصنة المعلومات. تجد هنا أيضًا إجابات على الأسئلة الشائعة. تابع نشرات المعلومات بشأن الحدث من مصادر موثوقة. تذكّر أيضًا أنه ليست كل المعلومات صحيحة التي يتم تداولها من خلال وسائل التواصل الاجتماعي. فلا تنشر الإشاعات ولا تنشر المعلومات الشخصية.

من أين أحصل على المعلومات؟

1

معلومات عن قرصنة المعلومات لمدينة هلسنكي

- تجد على صفحات الانترنت لمدينة هلسنكي من خلال الرابط **hel.fi/tietomurto** معلومات إضافية عن الحدث.
- خدمة الزبائن لمدينة هلسنكي للجهات التي تعرضت لقرصنة المعلومات، الاثنين - الجمعة، الساعة 8 - 18، هاتف 27139 310 09 أو **kaskotietoturvatilanne@hel.fi**
- مناوبة الطوارئ للأزمات لهلسنكي: الاثنين - الأحد على مدار الساعة، هاتف: 44222 310 09.

2

المساعدة بخصوص تسرب المعلومات على خدمة: Suomi.fi

الإرشادات التي نشرتها السلطات على خدمة Suomi.fi للجهات التي تعرضت لتسريب المعلومات **https://www.suomi.fi/oppaat/tietovuoto**

يتم الحديث في هذا الدليل عما يُفضّل فعله، إذا وقعت بياناتك الشخصية في أيدي غير أمينة. الدليل يقدم المشورة بخصوص ضحايا قرصنة وتسريب المعلومات ويُساعد إذا تعرضت لسرقة هويتك أو فقدت على سبيل المثال جواز السفر أو بطاقة الهوية.

3

بمَن من الممكن الاتصال إذا كانت قرصنة المعلومات تُثير القلق

مناوبة الطوارئ للأزمات لهلسنكي: الاثنين - الأحد على مدار الساعة، هاتف: 44222 310 09

هاتف الأزمات للجمعية المسجلة ميلي (Mieli ry)، الاثنين - الأحد على مدار الساعة، هاتف: 0111 2525 09

الأسئلة الشائعة بخصوص قرصنة المعلومات

ما هي قرصنة المعلومات في الواقع؟

قرصنة المعلومات تعني الدخول بدون إذن إلى منظومة المعلومات أو الخدمة أو الجهاز أو التطبيق، على سبيل المثال كاستخدام البريد الإلكتروني بدون إذن من خلال تعريفات تسجيل الدخول التي تم الحصول عليها. قرصنة المعلومات هي عبارة عن فعل يُعاقب عليه القانون قد تم تعريفه من خلال القانون الجنائي، كما أن محاولة قرصنة المعلومات فعل يُعاقب عليه القانون. مُجرد الدخول إلى المنظومة بغير إذن يستوفي المعالم التعريفية للجريمة، دون أن يكون هناك استغلال الجهة المستهدفة أو المعلومات المُستخدمة فيها.

ما هو الهدف من قرصنة المعلومات ومن الذي يفعلها؟

من الصعب تقييم دوافع قرصنة المعلومات. كثيرًا ما يكون في الخلفية السعي لتحقيق مكسب مادي. تُعتبر على سبيل المثال المعلومات المحمية في المنظومات ذات قيمة مادية. من الممكن أيضًا استغلال الوسط الذي تم اختراقه لنشر المواد الضارة أو من الممكن شل فعالية الوسط الذي تم اختراقه من خلال برامج الابتزاز الضارة. من الممكن أن يستخدم المهاجم الوسط الذي اخترقه كجزء من هجومات أخرى، على سبيل المثال أثناء الهجمات لإيقاف الخدمة.

من الممكن أن يكون دافع الفاعل على سبيل المثال التسبب بالضرر أو الابتزاز أو حتى التجسس على جهة حكومية. يقوم باقتراف قرصنة المعلومات المجرمون أو جهات حكومية أو حتى أشخاص عاديون. قرصنة المعلومات تتم بشكل مستمر، ولكن الأحداث الخطيرة نادرة.

كم قدر قرصنة المعلومات التي تتم محاولة القيام بها أو تتم ملاحظتها سنويًا في فنلندا؟

تتم ملاحظة الكثير من أحداث قرصنة المعلومات سنويًا. معظمها على كل حال عبارة عن عمليات اختراق غير ضارة تستهدف حسابات وسائل التواصل الاجتماعي أو سرقة التعريفات البنكية من خلال مختلف الحملات لاصطياد المعلومات.

كيف تغيرت عمليات قرصنة المعلومات خلال السنوات الأخيرة؟

التغيير الأكثر أهمية بخصوص قرصنة المعلومات هو أنه قد تطورت لدى الفاعلين القدرة على تصيد الرموز التعريفية المُتعددة المراحل، والتي يتم استغلالها لتسجيل الدخول. لقد تحسن الطابع اللغوي لحملات تصيد المعلومات من خلال استخدام الذكاء الاصطناعي.

لأي غرض تُستخدم المعلومات التي تمت سرقتها؟

من الممكن على سبيل المثال نشر المعلومات التي تمت سرقتها بدون إذن أو من الممكن ابتزاز صاحبها من خلال طلب فدية من الضحية. الاستخدام الإجرامي من الممكن أن يكون عبارة عن تسبب بالضرر أو ابتزاز أو تجسس.

عمليات قرصنة المعلومات التي تستهدف الشخص العادي من الممكن استخدامها على سبيل المثال في سرقات الهوية، حيث أنه يسعى شخص آخر خلالها للتظاهر بأنه هو الشخص الذي تعرض لقرصنة المعلومات. من الممكن أن تكون قرصنة المعلومات أيضا عبارة عن إزعاج تام. من الممكن التسبب بالإزعاج للشخص الذي تعرض لقرصنة المعلومات من خلال توقف المنظومة عن العمل وكذلك من خلال المعلومات الشخصية التي أصبحت في أيدي غير أمينة.

كيف من الممكن الحماية من قرصنة المعلومات؟

بخصوص الشخص العادي الطريقة الأكثر فعالية هي التعريف بالهوية المُتعدد المراحل وكذلك المعرفة العامة بأمن المعلومات. يُقصد بالتعريف بالهوية المُتعدد المراحل طريقة التعريف التكميلية لاستخدام تعريف المستخدم وكلمة السر لتعريف المستخدم بهويته عند الدخول للخدمة. طرق التعريف بالهوية التكميلية هي على سبيل المثال قوائم رموز المفاتيح التي تُستخدم مرة واحدة المستخدمة في البنوك عبر الإنترنت والرموز التي يتم إرسالها إلى الهاتف المحمول. يتوجب على المهاجم الذي حصل على الرمز التعريفي للمستخدم وكلمة السر أن يحصل أيضًا على الرموز التي تُستخدم مرة واحدة للتعريف بالهوية المتعدد المراحل كي ينجح في القرصنة.

استيلاء المُجرمين على البيانات الشخصية من الممكن أن يُثير قلقًا كبيرًا. من الممكن أن يُصبح الشخص ضحية لقرصنة المعلومات، حتى لو فعل كل شيء بشكل صحيح.

إرشادات مركز الأمن السيبراني للأشخاص العاديين للحماية من قرصنة المعلومات **(Ulkoinen linkki رابط خارجي)**

إرشادات مركز الأمن السيبراني للمنظمات/الجمعيات للحماية من قرصنة المعلومات (Ulkoinen linkki رابط خارجي)

ماذا يفعل مركز الأمن السيبراني لترافيكوم، ما هو دوره؟

مهمة فعالية CERT لمركز الأمن السيبراني أي مهمة الوضع المركزي هي الوقاية من انتهاكات أمن المعلومات واستيضاحها والإبلاغ عن أمور أمن المعلومات. يقوم CERT بتداول البلاغات المتعلقة بانتهاكات أمن المعلومات ويدعم المنظمات/الجمعيات التي قدمت بلاغًا لاستيضاح انتهاك المعلومات. كما أن مركز الأمن السيبراني ينشر المعلومات للمواطنين وكذلك يقدم المشورة من ناحيته بشأن ماذا بإمكان الفرد أن يفعله، إذا كانت معلوماته هدفًا لقرصنة المعلومات أو لتسريب المعلومات.

معلومات إضافية:

معلومات عن قرصنة المعلومات لمدينة هلسنكي (رابط خارجي Ulkoinen linkki)
نشرة معلومات لشرطة هلسنكي: تُجري الشرطة مُباحث بخصوص قرصنة معلومات واسعة النطاق لشبكة المعلومات لمدينة هلسنكي (رابط خارجي Ulkoinen linkki)
Tietovuoto.fi-opas (رابط خارجي Ulkoinen linkki)
مكتب مندوب حماية المعلومات (رابط خارجي Ulkoinen linkki)
خبر مركز الأمن السيبراني: قرصنة المعلومات - ما هي؟
إرشادات مركز الأمن السيبراني: هكذا تحمي نفسك من قرصنة المعلومات
تم تحديثه 2024/5/13