ICANN69 | الاجتماع الظاهري العام - تغييرات WHOIS بموجب قانون حماية البيانات العامة GDPR:
التأثير على المستخدمين النهائيين والسلامة العامة
الأربعاء، الموافق 21 أكتوبر 2020 – من الساعة 10:30 م حتى الساعة 12:00 بتوقيت وسط أوروبا الصيفي

[يجري تسجيل هذا الاجتماع]

أوزان ساهين: شكرًا لكم ومرحبًا بكم في جلسة تغييرات WHOIS بموجب قانون حماية البيانات العامة GDPR: جلسة التأثير على المستخدمين النهائيين والسلامة العامة التحضيرية. أنا أوازن ساهين، وأنا مدير المشاركة عن بعد لهذه الجلسة. يرجى العلم بأن هذه الجلسة يجري تسجيلها وتتبع معايير السلوك المتوقعة في ICANN.

أثناء هذه الجلسة، سيتم قراءة الأسئلة أو التعليقات فقط بصوت عال إذا ما تم تقديمها باللغة الإنجليزية في منصة الأسئلة الشائعة. يمكن الوصول إلى هذه الميزة من خلال شريط أدوات Zoom. سوف أقرأ الأسئلة والتعليقات بصوت عالٍ أثناء الوقت المحدد من قبل مشرف هذه الجلسة.

تشتمل هذه الجلسة على تدوين للنصوص والترجمة في الوقت الحقيقي. ولعرض النص المدون في الوقت الفعلي، انقر فوق زر "التعليق الخطي المصاحب" في شريط أدوات برنامج زووم Zoom. وسوف تشتمل الترجمة الفورية لهذه الجلسة على اللغة العربية والصينية والإنجليزية والفرنسية والروسية والإسبانية وسوف تُجرى باستخدام برنامج زووم Zoom ومنصة الترجمة الفورية عن بعد بإدارة شبكة المتخصصين في اتصالات الاجتماعات. نوصي الحاضرين بتنزيل تطبيق Congress Rental Network باتباع الإرشادات في غرفة دردشة Zoom أو من وثيقة تفاصيل الاجتماع المتوفرة على صفحة موقع الاجتماع على الويب.

إذا رغبت في التحدث، فيرجى رفع يدك في برنامج Zoom Room وبمجرد أن ينادي القائم على تسيير الجلسة اسمك، سيقوم فريق الدعم الفني لدينا بإلغاء كتم ميكروفونك. يُرجى ذكر اسمك للسجل واللغة التي ستتحدث بها إذا كنت تتحدث لغة أخرى غير الإنجليزية.

يرجى منك الحرص على كتم صوت جميع الأجهزة الأخرى بما في ذلك تطبيق Congress Rental Network عندما تتحدث. كما يُرجى التحدث بوضوح وبسرعة معقولة للسماح بترجمة فورية دقيقة.

أود التأكيد على أنه لنك يكون بمقدور المشاركين عن بعد النقر فوق زر الميكروفون وإلغاء كتم ميكروفوناتهم بأنفسهم أثناء هذا الاجتماع دون الحصول على المساعدة من فريق الدعم الفني.

وبالنسبة لجميع المشاركين في هذا الاجتماع، يمكنكم نشر تعليقاتكم في مربع الدردشة. للقيام بذلك، يرجى استخدام القائمة المنسدلة في مربع الدردشة أدناه وتحديد "الرد على جميع أعضاء اللجنة والحضور". فسوف يتيح ذلك للجميع الاطلاع على تعليقك.

برجاء ملاحظة أن المحادثات الخاصة متاحة فقط لأعضاء اللجنة في نسق ندوة الويب باستخدام برنامج زووم Zoom، وأي رسالة يتم إرسالها من أي عضو في اللجنة أو أحد الحضور المعتبرين إلى غيرهم لن يطلع عليها سوى مضيفو الجلسة ومساعدي المضيفين وأعضاء اللجنة الآخرين.

وبهذا، أحيل الكلمة إلى جوناثان زوك.

جوناثان زوك: شكرًا. معكم جوناثان زوك، نائب رئيس اللجنة الاستشارية العامة لعموم المستخدمين. لعلكم تعلمون جميعًا، فإن المجتمع الشامل قد تعامل نوعًا ما مع انتهاك نظام أسماء النطاقات DNS والمشكلات الأخرى ذات الصلة باعتبارها مسألة تخص الحملة لهذا العام، لكنني أشعر أن الكثير من هذه المحادثات كانت متكررة نوعًا ما ولم تصل إلى أي نتيجة محددة. وكان السبب الرئيسي في ذلك هو الافتقار للبيانات. هناك الكثير من الكلام المنمق موجه من جميع الجوانب وهو ما يجعل الحوار العقلاني حول هذه الموضوعات صعبًا للغاية.

وكثيرًا ما رأينا في سياق ICANN أن التنبؤات التي يتم إجراؤها في خضم شغف السياسة الجديدة لا تؤتي ثمارها في بعض الأحيان؛ لدرجة حدوث بعض النتائج الأخرى. على سبيل المثال، عندما تم اقتراح برنامج نطاقات gTLD الجديدة لأول مرة، اقترحت شركة Sony في جلسة استماع اعتماد بأنها ستستثمر 12 مليون دولار في عمليات التسجيل الدفاعية، وانتهى بهم المطاف إلى عدم تنفيذ ذلك. انتهى بهم الأمر إلى إيجاد طريقة أخرى للتعامل مع حماية علامتهم التجارية عبر نطاقات gTLD الجديدة هذه.

وبالمثل مع تطبيق قانون حماية البيانات العامة GDPR وما يترتب على ذلك من دعوة للاستيقاظ من مجتمع ICANN، كان هناك تدافع -- أليس كذلك؟ -- أدى إلى تنفيذ مواصفة مؤقتة، وتشكيل مجموعة عمل عملية وضع السياسات المعجّلة حول الكيفية يفترض أن تمتثل بها ICANN لأحكام قانون حماية البيانات العامة GDPR. ونتيجة لذلك، كان هناك تغيير جذري في البيانات المتاحة للجمهور عبر نظام WHOIS، وتم وضع نوع جديد من النظم التي تحتاجها الناس من أجل طلب معلومات من الأطراف المتعاقدة.

وهكذا في مسيرة عملية وضع السياسات المعجَّلة، كان هناك -وبغض النظر عن المآلات- نوع من مديري البيانات وطالبي البيانات الذين أصبحوا هذين الطرفين المهمين في تلك المناقشات.

ولذا فإن الفكرة من وراء هذه الجلسة العامة هي جمع هذه الأطراف معًا وإجراء مناقشة حول ما يحدث بالفعل خلال هذه الفترة المؤقتة. بمعنى آخر، ما هو مستوى طلبات البيانات التي يتم إجراؤها وكيف يتم التعامل معها. يبدو أننا غالبًا ما نتفاجأ من أن الأرقام أصغر مما نعتقد؛ وأنه لم يكن هناك الكثير من الطلبات أو لم يكن هناك الكثير من الشكاوى المقدمة إلى دائرة الامتثال التعاقدي، وما إلى ذلك. ولذا فإن البدء من أساس الوقائع يبدو وكأنه مكان أفضل للتواجد حيث نحاول إجراء محادثات حول بيانات المسجلين واستخدامها.

والأفضل من ذلك أن الأطراف التي كانت معنية بالأساسية بمسألة الوصول إلى بيانات المسجلين قد وجدت طرقًا بديلة للحصول على المعلومات من أجل إنفاذ العلامات التجارية، والقيام بأعمال جهات إنفاذ القانون وحماية المستهلك. ومن ثم فإنني أحاول

الوصول إلى حيث وصلنا الآن، أي عدة أعوام بعد ذلك، من حيث تلك البيانات والحاجة إليها وتوافره والفعالية التي يمكن الحصول عليها بها من خلال الطالبين من الأطراف المتعاقدة، وما إلى ذلك. وهذا ما نأمل الحصول عليه كمحادثة في إطار هذه الجلسة الجامعة، أي وهو في حقيقة الأمر مهمة التوصل إلى الحقائق حول ما وصلت إليه الأشياء اليوم، أي ما هو الوضع الراهن.

وهذا على أمل أننا سوف نحاول القيام بأقل قدر ممكن من النقاش الأيديولوجي وتعظيم دور مناقشتنا حول البيانات والحقائق حول طبيعة الوضع الراهن حاليًا.

ولكي يتم البدء في المحادثة، سوف نتحدث حول -- سوف نحصل على بعض وجهات النظر من أحد المجتمعات الطالبة، ألا وهي جهات إنفاذ القانون وحماية المستهلك. وفي سبيل ذلك، سوف أتيح عشر دقائق من أجل لورين كابين من المفوضية التجارية الفيدرالية وإلى غابرييل أندروز من أجل الحديث حول منظور جهات إنفاذ القانون، والحاجة إلى تلك البيانات، والبدائل التي تم طرحت نفسها، وكيف بدت العملية على مادر الأعوام القليلة الماضية.

وبهذا الكلام، أحيل الكلمة إليك، لورين.

شكرًا. وعليك إلغاء كتم الصوت.

لورين كابين: ما يزال الوقت مبكرًا بالنسبة لي، ومن ثم أرحب خصيصًا بكل من يعاني من مشكلة المنطقة الزمنية. وأنا متأكد من أن من لا يعانون من تلك المشكلة، أنكم ممتنون للغاية.

أنا لورين كابين، وأنا هناك من أجل تقديم منظور المستخدم النهائي لحماية المستهلكين حول كيفية استخدام الجمهور لنظام WHOIS.

هلا انتقلنا إلى الشريحة التالية، رجاءً.

وأما محامٍ لدى المفوضية التجارية الفيدرالية. وأنا في مكتب الشئون الدولية لحماية المستهلك ، وقد ركزت على هذه المشكلات، كما فعلت الوكالة التي أتبعها، على مدار عدة أعوام. لكن وجهات النظر التي سوف تسمعونها، فإنها تخصني أنا. وهي لا تعكس الموقف الرسمي للمفوضية التجارية الفيدرالية والتي تتحدث من خلال مفوضيها. ومن ثم فإنني أمثل نفسي فقط، بصفتي محامٍ أول في المفوضية التجارية الفيدرالية.

الشريحة التالية، رجاء.

كما أنني الرئيس المشارك لمجموعة عمل السلامة العامة، ولي باع في الدفاع عن هذه القضايا لفترة معقولة من الوقت.

إذن فإن المفوضية التجارية الفيدرالية لديها مصدر رائع حيث يمكن للمستهلكين والجمهور -ليس فقط في الولايات المتحدة ولكن أيضًا في جميع أنحاء العالم- تقديم الشكاوى عند الوقوع ضحية أو في حالة الشك في ممارسات خادعة أو احتيال أو غش. وهذا ما يطلق عليه اسم قاعدة بيانات حماية المستهلكين. وتقوم قاعدة البيانات تلك بجمع مئات الآلاف من الشكاوى كل عام وبها العديد من المساهمين من جميع أنحاء العالم.

ومما لا يدعو للدهشة، أنه عند النظر في تلك الشكاوى، يمكننا الحصول بشيء ما على صورة فوتوغرافية للكيفية التي يحصل بها الجمهور -أي شخص يدخل على الإنترنت من أجل شراء أشياء أو مقابلة أشخاص- على المعلومات، وكيفية استخدام الجمهور لنظام WHOIS، لأن الإشارات إلى نظام WHOIS صحيحة في شكاويهم.

إذن فإن ما قمت به هو أنني نظرت في شريحة من تلك الشكاوى، وعلى وجه الخصوص بعد تفعيل وسريان التغييرات التي أجريت على نظام WHOIS. وعندما أقول "تغييرات"، فإنني أقصد تلك التغييرات التي أخفت بعض المعلومات، وعلى وجه الخصوص معلومات جهة الاتصال الخاصة بالمسجل، أي الشخص المسئول. وإليكم ما توصلت إليه. أن المستخدمين النهائيين يستخدمون نظام WHOIS لأغراض متنوعة. ولكن بشكل أساسي فإنهم بصدد البحث عن مؤشرات للموثوقية. فهم يريدون النظر في سجلات WHOIS من أجل إجراء أعمال العناية الواجبة وأيضًا لمتابعة التصرفات

المريبة أو الضارة. ويريدون معرفة من هو المسئول. وفي بعض الأحيان يريدون محاول الاتصال بهم. وفي بعض الأحيان وأنا أعرف من خلال قراءة هذه الشكاوى أنهم يتحرون عن شيء شبيه بالغش، أي أنهم على الهاتف مع شخص ما يحاولون معرفة ما إن كانوا يتعرضون للغش أم لا. وهم ينطلقون إلى جهاز الكمبيوتر وينظرون في النطاق الذي قد يكون أدى بهم إلى هذه مكالمة الهاتف هذه.

وقد أشار المستهلكون في هذه التغييرات التي أجريت ما بعد WHOIS أن هناك معلومات مخفية أو ناقصة في السجل. وقد يفترضون أن شركة الأعمال غير أمينة بسبب نقص المعلومات. وقد يكون هذا الافتراض صحيحًا أو غير ذلك. وبالمناسبة، فإن المفوضية التجارية الفيدرالية تتلقى هذه الشكاوى. ولا يقومون بالتحقق من الشكاوى. بل يتلقونها فقط ويستخدمونها كنقطة بيانات.

ومن ثم فقد أشار الزملاء إلى أن التفاصيل قد تكون مخفية وأن ذلك يعوق جهودهم في إجراء العناية الواجبة. على سبيل المثال، قدم أحد الأشخاص شكوى تفيد بعدم وجود بيانات من أجل إحدى شركات المرافقة العامة. يمكنكم أن تروا من خلال هذا التمثيل الرسومي للكلمات الطرق التي يستخدم مختلف الأشخاص هذا، وهذه هي الألفاظ التي وجدتها في الشكوى -- في الشكاوى التي قمت بمراجعتها.

ولتوضيح الأمر أكثر، لأننا نحاول التحلي بالبلاغة هنا وليس أمامنا إلا -- لم يتبق إلا الوقت القليل. ولكن لكي أزيدكم من الشعر بيتًا -- الشريحة التالية من فضلك -- حول أنواع الخداع التي يستخدمها الناس من أجل التحري عن WHOIS: السلع المزيفة والخداع العاطفي والغش في الحيوانات الأليفة. وسوف تندهشون لعدد حالات الغش الموجودة في مجال عش الحيوانات الأليفة!

الشريحة التالية، رجاء.

غش الاختراعات، وأساليب التصيّد. وفي عصر فيروس كورونا، تعرضنا لحالات احتيال بالتصيّد من فيروس كورونا. وغش الدعم الفني، وحالات الغش والاحتيال باسم الحكومات، وعمليات الفحص المزيفة والاحتيال الوظيفي، مجموعة متنوعة كاملة.

كما أريد التأكيد على أن هؤلاء لا يستخدمون فقط معلومات جهة الاتصال في سجل WHOIS. وإلى ذلك الحد، فإن حظ هؤلاء عثر لأنه ما تزال هناك بعض المعلومات المفيدة، مثل وقت إنشاء النطاق والمكان الذي تم الإنشاء فيه. إذن هذه مجرد لمحة عن الطريقة التي يستخدم بها المستخدمون النهائيون بيانات WHOIS من أجل حماية أنفسهم بشكل أساسي، وهناك قدر من الإحباط تمت الإشارة إليه في هذه الشكاوى بأن بعض المعلومات غير متوفرة من أجل ذلك الغرض.

وسوف أحيل الكلمة الآن إلى زميلي غيب.

غابرييل أندروز: حسنًا. إذن الشريحة التالية، رجاءً.

عندما أتحدث، فإنني أتحدث سرديًا بالنيابة عن جهات إنفاذ القانون. وأنا أشير إلى أنه على الرغم من التماس الحصول على البيانات، فمن الصعب للغاية الحصول على أرقام جيدة من جهات إنفاذ القانون حول الأوقات التي تتضرر فيها بالوصول غير المتقن إلى نظام WHOIS.

وعلاوة على ذلك، سوف تميل جهات إنفاذ القانون إلى جمع وتوليف عدة مشكلات معًا. وقد لا يعرفون دائمًا أفضل من ذلك. ولكن سواء كان ذلك هو قانون حماية البيانات العامة GDPR أو قانون خصوصية المستهلكين في ولاية كاليفورنيا أو خدمة الخصوصية والبروكسي، في نهاية المطاف فإن ما يهم رجل الشرطة أو التحريّ أو مسئول السلامة العامة فعليًا هو أنهم يحاولون الحصول على إمكانية الاطلاع على البيانات والبيانات غير موجودة من أجل القيام بذلك.

والحديث حول واحدة من هذه المشكلات هو الحديث حولها جميع من منظور رجل الشرطة.

الشريحة التالية، رجاء.

أود أن أتعمق أكثر في المدة التي يستغرقها الأمر من أجل الحصول على البيانات. وهذا يهمنا. كما أن لها فترات مختلفة، أطر زمنية مختلفة، استنادًا إلى الظروف والملابسات.

ومن ثم كان السائد أن تكون لكم القدرة على إجراء بحيث عن الموارد العامة والحصول على معلومات المسجل في غضون عشر ثوان، أليس كذلك؟ إذن كان هذا ما اعتاد عليه رجال الشرطة استنادًا إلى خبراتهم السابقة في مجال التحقيقات.

وإذا لم يحصلوا على تلك البيانات، فربما لا يعلمون في الغالب حتى أنه يمكنهم اللجوء إلى أمين سجل من أجل الحصول على إمكانية الوصول إلى البيانات غير المخفية إذا ما كانت قد أُخفيت لأغراض قانون حماية البيانات العامة GDPR. وإذا لم تكن هناك خدمة خصوصية/بروكسي مفعلة وكان بإمكانهم أن يعرفوا بشيء ما أنه بإمكانه التواصل، فقد كانت الردود متنوعة. وسوف يستجيب بعض أمناء السجلات بشكل مباشر لطلبات إنفاذ القانون من أجل المعلومات المخفية، ونحن نعبر عن بالغ تقديرنا وامتنانا لذلك.

إذن سوف يكون الرد فقط على جهات إنفاذ القانون المحلية، بما يعني أن تكون الجهة هي نفس الهيئة الطالبة. وإذا لم تكن نفس أنت تلك الجهة، فربما لا يحالفك الحظ في تلك النقطة.

وقد يسأل البعض عن الإجراءات القانونية.

ولمصلحة المترجمين، إذا سمعتموني أقول "إجراءات قانونية" فإنني أني أمر محكمة أو مذكرة استدعاء، أو أي شيء من هذا القبيل.

كما أن الإطار الزمني لتلك الأشياء يتزايد لأقصى ما يمكن توقعه. وفي حالة رد أمين السجل تطوعيًا، فقد لا تتوفر الثواني العشر بعد ذلك ولكن قد تكن ساعات وربما أيام. وفي حالة اللجوء إلى الإجراءات القانونية، فأنت هنا بصدد توقع مدة ما بين أيام إلى أسبوعين في المتوسط من أجل الحصول على الإجراءات القانونية وتقديمها وتلقي الردود عليها.

وإذا لم تكن في نفس مكان الاختصاص القضائي وطالبتَ بإجراءات قانونية، فقد لا يحالفك الحظ أبدًا. ولكن يمكنك من الناحية النظرية -إذا كنت أحد الموقعين على معاهدة مساعدة

قانونية متبادلة- تقديم طلب معاهدة مساعدة قانونية متبادلة والحصول على البيانات في غضون ستة أشهر.

الشريحة التالية، رجاء.

ومن ثم عندما نتحدث حول التأثير، فقد أردت أن أستدعي واحدة من أكثر العمليات تأثرًا، وهي -- واحدة من أكثر مسئولياتنا تأثرًا ألا وهي إشعار الضحية. والمثال هنا يوضح نموذجًا على اختراق البريد الإلكتروني للشركات، وهو أحد عمليات الاحتيال الجنائية الأكثر انتشارًا على الإنترنت اليوم. فقد منينا بخسائر تقدر بنحو 23 مليار دولار جراء هذا العمل اعتبارًا في 2019، أي العام الماضي. وعلى ما يبدو أن الرقم يتضاعف كل عام. ولن أندهش إذا وصف الرقم إلى 50 مليار بنهاية هذا العام.

وفي هذا المثال، ترون الشخص المجرم ينتحل شخصية مدير تنفيذ بنطاق ceo@example.com مسجل. هذا نطاق مشابهة تمامًا، وفي بعض الأحيان تكون هناك كلمات متشابهة في الكتابة، حيث تكون موجهة خصيصًا إلى أحد الضحايا. وسوف يرسل بريدًا إلكترونيًا يطلب فيه تحويلاً بنكيًا. وهذه هي الطريقة التي تعمل بها تلك المخططات. فإذا صادف نجاحًا، تتم خسارة ملايين الدولارات. ونحن نجري -بصفتنا محققين في الماضي- عملية بحث عكسية في نظام أسماء النطاقات عن ذلك المسجل للنطاق الضار ونرى العديد من النطاقات الأخرى التي قام بتسجيلها. ويمكننا ربما أن نستشف من غالبية ذلك من هم الضحايا الفعليين لأنهم نطاقات مشابهة تمامًا، اتفقنا؟ وإذا أمكننا القيام بذلك بالسرعة الكافية، وإذا أمكننا التحرك بسرعة فعليًا، فقد تكون لنا القدرة عند ذلك على القيام بالمزيد من استعلامات نظام أسماء النطاقات حول تلك الضحايا ونحدد معلومات جهة الاتصال لهم ونتيح لهم معرفة الوقت الفعلي الذي يكونون فيه مستهدفين من قِبل أحد المحتالين.

والآن، حتى وإن كان هناك تأخير بسيط في إجراء عمليات البحث تلك بسبب وجود العديد من عمليات البحث طوال هذه العملية، فإنك تؤثر سلبًا على قدرتنا على إجراء تلك الإشعارات الهامة للغاية للضحايا لدرجة أنني لا أعتقد أن هذه الإجراءات لم تعد تُجرى بعد الآن. ليس هذا لأننا لا نحاول ولكن لأن الخطوة الأولى في الحصول على جميع هذه

النطاقات الإضافية المحتمل وقوعها ضحية، والتي تتطلب إجراءات قانونية والتي تتطلب بالتالي الآن أيامًا أو أسابيع.

وما يزال بإمكاننا محاولة ذلك. لقد أردت فعليًا أن أسلط الضوء على أن هذه من بين التداعيات في العالم الفعلي والتي تأتي من حالات تأخير طفيفة نسبيًا، تمضي من مجرد ثوانٍ إلى دقائق إلى أيام وإلى أسابيع. كما أن لها عواقب فرعية هائلة من المنبع. وأشير إلى أنني في الوقت المحدد والوقت نفيس، ومن ثم سوف أتحول إلى عضو اللجنة التالي.

جوناثان زوك: شكرًا لك، غابرييل. إذن بعد ذلك سوف نستمع من زملائنا في أبحاث أمن الفضاء الإلكتروني. غريغ آرون وليمان تشابن، تفضلا واقضيا على هذا الموضوع.

غريغ آرون: مرحبًا، أنا غريغ آرون.

الشريحة التالية، رجاء.

أجريتُ أنا وليمان مؤخرًا بحثًا حول التصيّد وحاولت اقتناص الكثير من المعلومات حول مقدار ما يحدث من ذلك، وما هو مكان حدوثها، وما إلى ذلك.

(لا يوجد صوت)

ونتج عن ذلك قرابة 300,000 رابط URL خاص بالتصيّد، وقد كانت هذه على 99,000 اسم نطاق وأكثر. بعد ذلك تبين لنا مكان استضافة تلك الأسماء. وقد نظرنا في توقيت وقوع هذه الأحداث وتبين لنا من هم أمناء السجلات، المستضيفين لموفري الخدمات المشاركين.

وما وجدناه أن التصيّد مركز إلى حد ما في حقيقة الأمر. وهي تتركز بالإضافة في أمكان في بعض نطاقات TLD. ويميل بعض موفري خدمات الاستضافة إلى الحصول على

كمية أكبر من آخرين. وإذا ما أردت الانتقال إلى رابط URL هناك، فيمكنك رؤية نتائج الدراسة.

ومن الأشياء التي نراها هو أن نطاقات التصيّد تُستخدم سريعًا. والغالب -- وغالبيتها تستخدم في غضون 14 يومًا من إنشاء النطاق، والبعض منها، بل الكثير منها في غضون ثلاثة أيام من إنشائها.

كما رأينا أن التصيّد والاحتيال مشكلة أكبر مما هو معلن. ففي كل مرة تتم فيها إضافة مصدر جديد للبيانات، تكتشف حالات تصيّد جديدة لم يعرف الآخرون عنها شيئًا.

كما أن هناك أساليب مراوغة يستخدمها المجرمون.

وعندما تنظرون في هذه البيانات، يمكنكم اكتشاف ربما ما هي الخلفية والأساس وراء المشكلة، لكن لا يمكنكم إقرار وتحديد سقف ما يحدث.

ومن بين الطرق التي نعرفها حول مقدار التصيّد الموجود هو من خلال معرفة مقدار المعلن والكتلة المدرة، وهي -- محاولة معرفة هذه الأشياء -- ونحن نبحث وفي بعض الأحيان يكون الأمر صعبًا. وقد تداخلت الكثير من هذه المصادر بمقدار ضئيل للغاية. كما أننا لا نرى التصيّد في بعض المناطق على مستوى العالم. وهناك نقص واضح في البيانات حول التصيّد والاحتيال في أماكن مثل الصين وروسيا بسبب الإبلاغ والإعلان.

إذن من بين تلك العوامل التي تؤثر على قدرتنا على العثور على التصيّد هو الافتقار إلى معلومات WHOIS. ثمة مشكلتين. الشريحة التالية.

بالطبع عندما تحاولون معرفة مدى كبر العضو، فهذا يتوقف على ما تقوم بقياسه والطريقة التي تقيس بها. فشركة Google على سبيل المثال، مهتمة بالمقاييس لأنه يمكنهم في حقيقة الأمر التعرف على مقدار التصيّد الذي يقومون بحجبه في المتصفِّح Chrome. وهذا من المقاييس الهامة للغاية. وهذه الشريحة من برنامج التصفح الآمن المقدمة منهم، ويوضح اللون الأحمر عدد مواقع التصيّد التي كانوا يحجبونها. الأمر شائق لأن لديهم طريقة متسقة على مدار فترة زمنية طويلة.

ما ترونه هو تصاعد وتيرة التصيّد. وفي الوقت ذاته، هناك تراجع في البرمجيات الضارة. وليس هذا غير معتاد بالضرورة. فمقدار الجريمة الإلكترونية ومكان حدوثها يميل إلى التحول والتغير بمرور الوقت. فمن بين أسباب تراجع البرمجيات الضارة هو أنه كانت هناك بعض شبكات بوت نت التي انخفضت. والسبب أيضًا يرجع إلى أن المجرمين أقل اهتمامًا بتشغيل بعض أنواع البرمجيات الضارة الخاصة بالمصارف. وعوضًا عن ذلك، فقد تحولوا إلى أنواع أخرى من الجريمة، والتي تشمل عمليات اختراق البريد الإلكتروني للشركات التي تحدث عنها غيب للتو.

وعندما تحاولون فهم مقدار الجريمة الموجود بالفعل، فإن هذا يتوقف على طبيعة ما تقومون بقياسه وكيفية قياسه، كما يتوجب عليكم أيضًا النظر إلى الصورة الأكبر. وإذا تجروا قياسًا لبعض الأشياء، فلن تتوصلوا ببساطة إلى أي معلومات عنها.

الشريحة التالية، رجاء.

والآن، ما السبب في ضرورة الحصول على معلومات WHOIS؟ إننا بحاجة إلى المعلومات لأننا نريد معرفة الكثير من الأشياء مثل موعد تسجيل أي اسم نطاق وأمناء السجلات الذين تم التسجيل لديهم. وهذه المعلومات غير حساسة. وقد رأينا أن تاريخ التسجيل مهم حقًا.

ومن بين المشكلات التي نواجهها في الوقت الحالي هو تقييد المعدل. وهذا يعني أن مشغلي السجلات وأمناء السجلات يتيحون لك فقط إجراء عدد محدد من الاستعلامات في غضون فترة زمنية محددة. وقد كتبت اللجنة الاستشارية للأمن والاستقرار في ICANN ورقة بحثية حول هذا الأمر. وهي تمنعنا من الحصول على المعلومات غير الحساسة التي يمكن أن تتيح لنا رؤية وربما اكتشاف المزيد من هجمات التصيّد.

كما أن من يحاولن محاربة المشكلة ينظرون -أو اعتادوا النظر في- معلومات جهة الاتصال في دفتر التسجيلات. وقد كان هذا الأمر هامًا لأن المجرمون كثيرًا ما يقومون بتزييف المعلومات، ولعلكم تتخيلون ذلك. ولا يقدمون أي معلومات دقيقة حول جهة

الاتصال. ومن الممكن إجراء عمليات فحص على ذلك، وإذا لم تكن صحيحة، فهذا يعد مؤشرًا على سوء النية من جانب المسجل.

كما أنها قد أتاحت لنا معرفة ما إن كان طرف ما قد قام بتسجيل أكثر من اسم نطاق واحد، ويمكنكم إجراء بعض عمليات البحث ومقارنة المعلومات. ولم يعد الأمر مفيدًا بعد الآن في عالم ما بعد قانون حماية البيانات العامة GDPR.

لكن ما رأيناه في تقريرنا أكد شيئًا عرفناه على مدار فترة زمنية طويلة، ألا وهو معرفة أنه عندما يقوم المجرمون بتسجيل اسم نطاق واحد فإنهم غالبًا ما يقومون بتسجيل مجموعة، وهناك أمر نشاهده وهو أن تلك المجموعات لا يتم التعرف عليها كما كان في الماضي. ففي بعض الأحيان يمكننا رؤية سلاسل طويلة متتابعة من أسماء النطاقات، وقد تم اكتشاف القليل منها ووضعه في القائمة السوداء، لكن يمكنكم معرفة أيها كان مفقودًا.

الشريحة التالية رجاءً.

من بين الأشياء الأخرى التي ننظر فيها هي طول هجمات التصيّد. وهي تمثل قدرًا كبيرًا من البيانات الرائعة التي قام المعنيون في شركة PayPal وشركة Google وفي جامعة ولاية أريزونا بتجميعها. لقد كانت في حقيقة الأمر دراسة هامة أجريت هذا العمل ونواة لدراسات أخرى. وقد كان لتلك الشركات رؤية رائعة إلى حد ما لأنه يمكنهم معرفة من هم الأشخاص الذي يجرون عمليات النقر بالماوس ويمكنهم تتبع أشياء بدءًا من أول زيارة إلى موقع خاص بالتصيّد وصولاً إلى آخر الزيارات، وبعد ذلك إذا كانت عملية تصيّد تشتمل على شركة PayPal، فيمكنهم معرفة الأشخاص الواقعين فريسة لهذه العمليات وكم عدد من فقد منهم أموالا من حساباتهم، وما إلى ذلك.

وقد كانت تلك البيانات متسقة إلى كبير مع الدراسات الأخرى، بما في ذلك بعض الدراسات التي أجريتُها، لكنها توضح لنا أن هجوم التصيّد قصير.

فبحلول الوقت التي تحصل فيه على زيارتك الأولى وصولاً إلى وقت اكتشاف التصيّد بشكل ما، ربما من خلال أحد الأطراف، تنقضي مدة ثمانية ساعات تقريبًا، وغالبًا ما

يحدث هجوم التصيّد بالكامل على مدار ما يقرب من 17 أو 18 ساعة. إذن بحلول الوقت الذي يتم فيه اكتشاف هجوم التصيد في المعتاد، يكون القسم الأكبر من الضرر قد وقع. ويكون غالبية الضحايا قد دخلوا إلى الموقع، ومن سيفقدون في حقيقة الأمر أموالاً جراء الاحتيال قد وقعوا بالفعل ضحية لذلك.

الشريحة التالية رجاءً.

ومن الأشياء التي اكتشفناها أيضًا هو أن قرابة 60% من النطاقات المستخدمة في هجمات التصيّد مسجلة بمعرفة متصيّدين.

والنطاقات المستخدمة في التصيّد تنقسم إلى فئتين. الأولى وفيها يقوم المتصيّدون بشراء أسماء نطاقات وبعد ذلك يستخدمونها من أجل إطلاق مواقعهم المزيفة. ويمكن للمتصيّدين أيضًا استخدام أسماء النطاقات التي اقتحموها بالفعل من أجل الاستضافة، ومن ثم يمكنهم في حقيقة الأمر القيام بالتصيّد على اسم نطاق يخص شخص آخر، أي طرف بريء.

ما نود القيام به بصفتنا جهات رد واستجابة هو أننا نريد أن يكون هناك اهتمام بتلك الأنواع من المواقع في موفر الخدمة المستضيف، والإبقاء على بقية المحتوى، ومنع أي ضرر جانبي من الحدوث لذلك المسجل البريء.

وعلى الرغم من ذلك، فإن أسماء النطاقات المسجلة من خلال متصيّدين، فيمكن وقفها عن العمل دون أي نوع من الأضرار الجانبية.

وقد اكتشفنا -من خلال منهجيتنا- ما يقرب من 60% من أسماء النطاقات مندرجة تحت هذه الفئة المسجلة بشكل ضار.

فريق من شركة SIDN Labs ومن الجمعية الفرنسية للتعاون في مجال تسمية الإنترنت -- ومن هم في نطاق NL. مشغلي سجل FR -- قاموا بإنشاء نظام منفصل. وكان هناك القليل من التداخل في طرائقهم. وقد قاموا بإنشاء نظام تفصيلي، وتوصلوا إلى نسبة 57%. ومن ثم فقد اقتربنا إلى حد ما في النسب، وقد أجروا عملاً جيدًا للغاية وهو ما اعتبرته ممتعًا للغاية.

الشريحة التالية. إذن أعتقد أن بعض المزايا هي هذه الأشياء. وما نجده هو الكثير من عمليات التسجيل بغرض الإساءة، ومن الصعب علينا الآن معرفة ذلك. وأحد الأسباب هو أنه ليس لدينا بعض البيانات التي كانت متاحة في السابق وهذا يعد نتيجة واضحة بشيء ما.

وبشكل ما، تكون بيانات جهة الاتصال من الأشياء التي تميز اسم نطاق عن غيره. وهو مؤشر على سوء النية. وبشكل واضح فإن من يقوم بتسجيلها أو من يبدو أنه مسجلها يمثل معلومة هامة بشكل واضح.

وإليكم خبر سار إن جاز التعبير، ألا وهو أنه ما يزال بإمكان أمناء السجلات ومشغلي السجلات الوصول إلى تلك البيانات. ويمكنهم رؤية ذلك حتى وإن لم يتمكن آخرون من ذلك.

ونظرًا لأن الكثير من أعمال التصيّد تتم من خلال المتصيّدين أنفسهم ممن يقوم بتسجيل أسماء النطاقات تلك، فثمة فرصة لأمناء السجلات ومشغلي السجلات بمواصلة الاستفادة من تلك البيانات. وما نراه على الرغم من ذلك هو أن هناك تصيّد مستمر مرارًا وتكرارًا فيبعض نطاقات TLD وبعض أمناء السجلات.

أما فيما يخص عملية وضع السياسات المعجَّلة، تمثلت إحدى النتائج في أننا سوف نحصل على وقت كافي مستهدف من أجل طلبات الحصول على البيانات. علمًا بأن طلبات الأمن المعلوماتي كما في طلبات التصيّد منصوص عليها في قانون حماية البيانات العامة GDPR نفسه. ويطلق عليها لفظ المصالح المشروعة من أجل طلب الحصول على البيانات.

وعلى الرغم من ذلك، فإن مدة خمسة أيام وبعد ذلك ربما قد تكون لمدة عشرة أيام، سوف يكون هذا أمرًا غير فعال نظرًا لأن هجمات التصيّد تدوم لفترات أقل -- تدوم لأقل من يوم واحد.

ومن ثم فإن البيانات التي تأتي من خلال نظام الوصول/الإفصاح القياسي قد تأتي سريعًا وقد تأتي ببطء، ولن تكون الطلبات البطيئة مفيدة في المشكلات الفورية.

إذن فالتصيّد تمثل حالة اختبار رائعة مؤهلة للأتمتة. وهذا من الأشياء التي سيتوجب على فريق التنفيذ النظر فيها. ولكن إذا كان من الممكن تحويلها إلى روتين، فقد تكون لنظام الوصول/الإفصاح القياسي القدرة على توفير بعض البيانات المفيدة للرد على التصيّد والاحتيال والحد من الوقوع ضحية له.

شكرًا.

جوناثان زوك: شكرًا لك، غريغ.

أعتقد أن مارك لم يشترك معنا إلى الآن في الاجتماع. هل ذلك صحيح؟

>> هذا صحيح.

جوناثان زوك: حسنًا. إذن أود أن أواصل العمل وأنتقل إلى ميلتون بحيث يمكننا الدخول في النقاش بما أن هناك وبشكل واضح مناقشة رائعة للغاية تجري الآن. إذن فلنقم باستعراض هذه العروض التقديمية الأولية ونبقي على مواصلة الحوار.

إذن، ميلتون، تفضل رجاءً.

ميلتون مولر: تحياتي للجميع. أنا ميلتون مولر. أنا أستاذ في معهد جورجيا للتكنولوجيا بالولايات المتحدة. وبالمناسبة، جميع من في هذه اللجنة من الولايات المتحدة. أليس هذا مدهشا؟

في حقيقة الأمر، كانت مناظرات WHOIS مرتكزة بشكل ما على هذه الفروقات بين أوروبا والولايات المتحدة بخصوص قانون الخصوصية.

هل يمكنني الانتقال إلى الشريحة التالية، رجاءً.

وإليكم شيء ما تسمعوه كثيرًا إلى الآن، ألا وهو سبب حضوري في هذه اللجنة، وأنا في حقيقة الأمر أتحدث حول حقوق ومصالح المسجل، أي الشخص الذي يسجل اسم النطاق. ولا يجب أن يكون من الصعب جدًا فهم السبب وراء اهتمام ومصلحة من يسجلون النطاقات بإخفاء بعض المعلومات الشخصية، أو المعلومات الشخصية الحساسة. فموجب العديد من قوانين الخصوصية، فإن لديهم في حقيقة الأمر حق قانوني، بالإضافة إلى مصلحة في الحفاظ على تلك البيانات.

وفي حقيقة الأمر، لدى المفوضية التجارية الفيدرالية -التي تعمل فيها لورين- الكثير من المعلومات حول كيفية عدم إتاحة معلومات مثل عنوان البريد الإلكتروني وغيرها من البيانات المحددة لهوية أصحابها مثل رقم هاتفك المحمول عبر الإنترنت متى ما كان بإمكان أي أحد نسخها واستخدامها. وبالطبع، فإن كل ما قمنا به فعليًا فيما يخص إنفاذ قانون حماية البيانات العامة GDPR على نظام WHOIS هو استخدام تلك الفكرة العقلانية الشائعة بأن المجرمين والمنتهكين بإمكانهم إساءة استخدام المعلومات المحددة لهوية أصحابها. ولا يفضل بشكل عام إتاحة عنوان بريدك الإلكتروني وعنوانك المادي بشكل عشوائي لأي أحد ولكل أحد على الإنترنت.

وعلى الرغم من ذلك، في نظام WHOIS الحالي، بالطبع، ما تزال هناك القليل من المعلومات: اسم المسجل والدولة، وفي بعض الحالات أيضًا اسم الولاية واسم المدينة موجودان. ونحن نأمل أن نكون قد أعددنا طرق جديدة فعالة من أجل الإفصاح عن البيانات المخفية بطريقة تكون أسرع.

وأنا متشوق لمعرفة السبب وراء عدم اهتمام المجتمع الشامل أكثر بحقوق مسجل اسم النطاق. وأنا أعرف أنه من المفترض بهم تمثيل المستخدمين. وأود أن أعرف ما هو الموقف الذي كانت عليه هياكل المجتمع الشامل الأوروبية فيما يخص نظام WHOIS. لأننا لم نسمع بالتأكيد أي دعم بالنسبة للامتثال بقانون حماية البيانات العامة GDPR من اللجنة الاستشارية العامة خلال عملية وضع السياسات المعجَّلة.

الشريحة التالية، رجاء.

والآن، لقد أحببت العرض المقدم من جوناثان على اللجنة، فهل بإمكاننا محاولة الحديث حول الحقائق هنا. إذن من غير السهل الحصول على معلومات شاملة حول ما قد جرى. لكنني نركز تمامًا على حقيقة أننا لا نتحدث حول ما إن كان التصيّد سيئًا وما إن -- والطريقة التي يعمل بها، بنفس مقدار حديثنا حول الطريقة التي تعمل بها هذه الأشياء قبل وبعد إخفاء البيانات بسبب امتثالنا لقانون حماية البيانات العامة GDPR.

لذلك إذا ما نظرنا في إحصائيات شركة Google التي عرضها علينا غريغ ونظرتم من 15 ديسمبر/كانون الأول إلى مايو/أيار 2018، وهي الفترة -- هي فترة 17 شهرًا بشكل أساسي قبل سريان عمليات الإخفاء، ونظرتك في مدة 18 شهرًا أو 17 شهرًا بعد أن سرت عمليات الإخفاء، فيما يخص مواقع البرمجيات الضارة، فسوف ترون انخفاضًا قبلها وبعدها. في حين كان الانحدار بعدها أكبر بكثير بشكل واضح.

وإذا ما نظرنا في مواقع التصيّد، فسوف ترون زيادات كبيرة للغاية قبل وبعد تنفيذ عمليات الإخفاء.

كما أنني نظرت في بعض بيانات البريد غير المرغوب، على الرغم من الصعوبة الشديدة في الوصول إلى بيانات بريد إلكتروني غير مرغوب طويلة الأجل. ومرة أخرى، لا ترون أي راب فيما بين إخفاء البيانات في 2018 وحكم ونطاق المشكلة. ومن غير الممكن تحديد أي نوع من الروابط الإحصائية بين عمليات الإخفاء وأنواع التغيرات في المشكلة.

ومن ثم أعتقد -ولعلكم تعلمون- فإن الحالة التي يمكنكم إجراؤها استنادًا إلى البيانات ما بين الإخفاء ومشكلات الجريمة الإلكترونية لدينا هو رابط ضعيف للغاية.

ولا يرجع السبب في ذلك إلى أنه من غير المفيد بشكل واضح في بعض الحالات بالسنبة لجهات إنفاذ القانون الحصول على وصول سريع لهذه البيانات. وبشكل واضح، فإنها كذلك. وأيضًا حقيقة أن ذلك الوصول السريعة يمثل عامل تهديد، وجزء من سبب المشكلة. وأيضًا حقيقة أنه كلما زات عمليات التصيّد أكثر وأكثر وزادت التسجيلات المسيئة أكثر

وأكثر زاد تعلم المجرمين كيفية تزييف المعلومات ويتوصلون إلى طرق أكثر مهارة في الإسناد الترافقي والحصول على معلومات هوية زائفة في ذلك دون أن يكون من السهل لمن يبحثون في بيانات WHOIS اكتشافها.

وثمة ملاحظة أخيرة في هذه المشكلة الخاصة بالتصيّد، اسمحوا لي أن أقول بأنني عندما أقوم بتدريس أمن الفضاء الإلكتروني للطلاب في معهد جورجيا الفني، نجري تدريبات نقوم يكون لدينا فيها فرق مكونة من خمسة طلاب يقومون بصناعة بريد إلكتروني للتصيد ويرسلونه إلى معلميهم ويرون إن كان بإمكانهم خداعهم. ومن بين الأشياء التي اكتشفوها، أي التي اكتشفها الطلاب هو أن نطاقات التصيّد غالبًا ما يتم اكتشافها من خلال خوارزميات متنوعة بين الشركات المضيفة، من بين أفراد الويب، الشركات المصنعة لبرامج التصفح التي تستخدم أشياء مثل ما مدى سرعة تسجيله وما هو أحدث نطاق وهل يتطابق مع بعض السلاسل أم لا. وربما ما يقرب من نصف هؤلاء الطلاب يكتشفون أنهم -- أن نطاق التصيّد الخاص بهم محجوب حتى قبل أن يتمكنوا من إتمام الاشتراك وإرساله لي.

الشريحة التالية، رجاء.

مرة أخرى، ليس أننا قمنا بإلغاء الوصول إلى هذه المعلومات بالكامل. بل إننا أسسنا في عملية السياسة الجديدة نموذجًا مركزيًا ومعياريًا من أجل تقديم طلبات الإفصاح. وأعتقد أنه يتوجب علينا أن نفهم -ولا يمكننا أن نتجاهل ذلك- أن هذا الأمر يتعلق برمته بالامتثال. وهذه ليست مسألة اختيارية؛ اتفقنا أيها الزملاء؟ حيث يجب علينا الامتثال للقانون. ما قمنا به من خلال الجهود الدؤوبة في عملية وضع السياسات المعجَّلة هو التوصل إلى آلية للإفصاح تكون متوافقة مع قانون حماية البيانات العامة GDPR، وهذا يعني أن العديد من الطلبات يجب أن تخضع ببساطة للمراجعة من أجل التأكد مما إن كانت هناك أي مصلحة مشروعة وما إن كان الطالب مرخص له وما إلى ذلك.

إذن سوف نترك الأمر عند هذا الحد، ونتطلع إلى إجراء مناقشة قوية مع أعضاء اللجنة الآخرين ومع الجمهور.

شكرًا لكم على الاستماع.

جوناثان زوك: شكرًا جزيلاً لك، ميلتون. معكم جوناثان زوك مرة أخرى، للعلم والإحاطة. وأريد التأكيد على شيء قاله ميلتون وهو من الأشياء التي ربما تكون قد حدثت وهي تتعلق بالامتثال للقانون. ومن ثم كما نناقش هذه المسألة في المستقبل، فأعتقد أننا نريد أن ننظر فيما يبدو عليه العالم في الوقت الحالي، في ظل هذا القانون، وليس لإعادة الخوض في إجراءات ما إن كان القانون مناسبًا أو أي شيء من ذلك القبيل، ولكن عوضًا عن ذلك، ما هو نوع علاقة تدفق البيانات الموجودة بين طالبي البيانات وحائزيها. هذه هي الفكرة في حقيقة الأمر. وليس الهدف هو إجراء نفس الحوار الذي أجراه فريق عملية وضع السياسات المعجَّلة على مدار عامين مرة أخرى، بل نعيد النظر فيما كانت عليه العملية منذ ذلك الحين وما تبدو عليه تلك العلاقة.

وللحديث حول ذلك، أعتقد أن أوين سيكون الأمثل. فقد قاموا للتو بإعداد تقرير حول الطلبات الأخيرة المقدمة للحصول على البيانات. ولا أتذكر في أي تاريخ كان ذلك. وثمة ندوة عبر الويب من الجدير التحقق منها. أعتقد أن أوين سوف يستعرض معنا هذه المسألة ويعطينا ملخصًا بشكل ما حوله هنا ويتحدث قليلاً من جانب أصحاب البيانات في هذه المعادلة فيما يخص ما كان عليه الأمر منذ تنفيذ المواصفة المؤقتة وما كانت عليه السنوات القليلة الماضية.

أوين، عليك بهذا الموضوع، رجاءً.

أوين سميغلسكي: شكرًا لك، جوناثان.

لنرى. أنا أظهر -- الفيديو يعمل لكنني لا أظهر على الشاشة، أو هل يمكن للجميع رؤيتي؟

أوزان ساهين: مرحبًا بك، أوين. نعم، يمكننا رؤيتك.

جوناثان زوك: نعم، يمكننا رؤيتك وسماعك أيضًا.

أوين سميغلسكي: حسنًا، رائع. اعتدت أن أرى نفسي لكن ليس -- لا بأس. الشريحة التالية.

إذن أنا أوين سميغلسكي. وأنا أعمل لدى أمين السجل Namecheap. كما أنني نائب رئيس شعبة السياسات لمجموعة أصحاب المصلحة في أمناء السجلات. والمادة التي سوف أقدمها لكم عبارة عن إصدار مختصر من ندوة عبر الويب قامت السجلات وأمناء السجلات بتجميعها في سبتمبر/أيلول. وثمة رابط إلى ندوة الويب، أو العرض التوضيحية، بالإضافة إلى التسجيلات حول تقويم منظمة دعم الأسماء العامة. وقد وضعت الرابط في الشرائح هنا بحيث يمكن للجميع الاطلاع وإلقاء نظرة عليها. ومن ثم فإنني أدعوكم إلى إلقاء نظرة والمراجعة لأن هناك الكثير من المعلومات موجودة هناك.

وقد شاركت في ندوة الويب تلك بالإضافة إلى ثلاثة من الزملاء ممن قاموا بتجميع المعلومات التي سوف أعرضها عليكم الآن: آلان وودز من سجل Donuts، وبيث بايكون من سجل المصلحة العامة، مشغل نطاق org.، وسارة وايلد من أمين السجل Tucows. إذن يتوجب أن أعترف بكل الفضل لهم في غالبية المادة التي سوف أعرضها عليكم هنا.

الشريحة التالية، رجاء.

أعتقد أن هناك شيء مفقود في الكثير من هذه المناقشة ألا وهو قانون حماية البيانات العامة GDPR وحماية البيانات ليست شيئًا جديدًا. وتعود جذور هذه الأشياء إلى نهاية الحرب العالمية الثانية، والتخوف السائد خلال تلك الفترة، المعلومات الشخصية للأشخاص كانت تستخدم من أجل إعداد ملفات للعديد من المجموعات واستهدافها من الدول ومن الجهات الفاعلة الأخرى. وقد اشتمل ذلك على الأسماء والأديان والمنشأ العرقي والتوجه الجنسي وغيرها من العوامل. وبعد مضي تلك الفترة وما بها من أهوال، فإن الاهتمام بالخصوصية في حماية البيانات الشخصية استحوذ على أهمية كبيرة للغاية، واستمر ذلك حتى يومنا هذا. وهذا هو السبب في أن حماية أصحاب البيانات يمثل مسألة

هامة وما السبب في أنها شيء لا يمكن التغاضي عنه هو أن بعض الناس يدركون أنهم يتعرضون للمضايقات في بعض الأحيان. ومن ثم فقد تم تضمين هذه المسألة في الإعلان العالمي لحقوق الإنسان في عام 1948. وجاءت بعد ذلك المزيد من المعاهدات والاتفاقيات، وكان أول قانون لحماية البيانات في السويد في 1973، وجاءت عشرات الاتفاقيات والمعاهدات بعد ذلك قبل إنشاء ICANN في عام 1998.

الشريحة التالية، رجاء.

إذن هناك سبعة مبادئ حاضرة وموجدة في قوانين حماية البيانات الأوروبية، ويجب أن تُقرأ جميعها مع الأخذ في الاعتبار حماية صاحب البيانات وليس بالضرورة أمام الأطراف الأخرى فيها. ومن ثم لن أستعرضها هنا، ولكن البعض منها هو ما يجب أن يكون لديكم فيه غرض محدد وهو جمع هذه المعلومات. وينبغي عدم تناول المزيد من المعلومات بأكثر من اللازم. ويجب عليكم التأكد من أنه تُخزّن لفترة زمنية محددة. ويجب أن تتم بطريقة آمنة. ويجب أن تكون هناك مساءلة عن تلك البيانات.

وقبل تاريخ سريان قانون حماية البيانات العامة GDPR، فإن الوصول غير المقيد إلى بيانات التسجيل من خلال نظام WHOIS قد خالف العديد من هذه المبادئ.

الشريحة التالية، رجاء.

ومن ثم فإن هذه ليست سوى نظرة عامة تسلط الضوء على بعض المشكلات هنا أو بعض النقاط. ولعلكم تعلمون، فإن قانون حماية البيانات العامة GDPR ليس جديدًا. ولعلكم تعلمون، كانت هناك بعض التغييرات التي أجريت عليه من أجل زيادة مستوى المسئولية، ولكن ما تم تفعليه من خلال قانون حماية البيانات العامة GDPR كان حاضرًا في أوروبا بالإضافة إلى دول أخرى ومعاهدات على مدار عقود قبل ذلك.

ولم يتم إلغاء نظام WHOIS أبدًا. فهو ما زال موجودًا. كل ما هنالك أنه يتوافق مع القانون. وأنا أعلم أنه تم تكرر في هذه الجلسة عدة مرات الآن أن بيانات WHOIS لازمة من أجل إيقاف التقارير. وليست هذه هي الطريقة الأفضل للقيام بذلك. وأفضل طريقة هي تقديم

التقارير إلى أحد الأطراف المتعاقدة، سواء كان أمين سجل أو سجل أو مباشرة إلى أحد موفري خدمات الاستضافة. فهؤلاء هم من بإمكانهم الاهتمام بهذه المسألة. ويجب عليكم إجراء تحليل بعد ذلك من أجل معرفة من كان يقوم بماذا وكيفية منع ذلك، بعدئذ يمكن القيام بذلك بعدها عند الانتهاء من الوقت المحدد لكي يتوقف هجوم تصيّد.

والتقارير والعروض التقديمية لا تفيد في حل المشكلة. ونحن بحاجة للحصول على تقارير حول ذلك من أجل أن نتمكن من اتخاذ الإجراءات.

ومرة أخرى، جميع هذه القوانين الخاصة بحماية البيانات، بما في ذلك قانون خصوصية المستهلكين في ولاية كاليفورنيا والبرازيل لديها قانون للخصوصية وغيرها من الدول التي ما تزال تظهر وتعطي الحقوق لأصحاب البيانات. وهي لا توفر أي حق إلى جهة أخرى من أجل الوصول إلى تلك البينات ولا تفرض أي التزام بالإفصاح عن تلك البيانات.

فبيانات WHOIS غير المخفية من قبل وفرت عوامل هجومية كان مجتمع ICANN يتعامل معها على مدار ما يزيد عن عشر سنوات. قرصنة النطاقات والبريد غير المرغوب والتصيّد وانتحال الهواتف وإشعارات التجديد الزائفة. كل الأشياء التي كنا نتحدث حولها على مدار أكثر من عقد هي الأشياء التي يمكن التعامل معها وحلها من خلال حماية بيانات التسجيل من إمكانية وصول الجميع إليها بالكامل.

ومرة أخرى، وكما سمعنا مرات ومرات، فإن الانتهاك الكلي لأسماء النطاقات ليس في تصاعد. بل آخذ في التنازل. ولم تكن هناك أي زيادة كلية خلال جائحة مرض كوفيد-19.

التالية رجاءً.

ومن ثم فإنني أطرح هذا الأمر هناك من باب التوضيح. أما بالنسبة لمن هم مهتمون بتوفير طلبات الحصول على البيانات، فهذا هو الحد الأدنى من أفضل المعلومات التي يمكن لأي أحد أن يقدمها إلى أمين سجل أو سجل عند تقديم طلبات الإفصاح عن البيانات. وهو يستند إلى التقرير النهائي للمرحلة الثانية لعملية وضع السياسات المعجَّلة بالإضافة إلى أفضل الممارسات التي قام على وضعها أمناء السجلات والسجلات. وثمة رابط، أو

رابط مباشر إلى هذا الأمر في موقع مجموعة أصحاب المصلحة في أمناء السجلات على الويب وقد وضعته هناك. لكنها توفر فقط الحد الأدنى من المعلومات الأساسية التي سوف يحتاج أي طرف آخر مراجعتها من أجل إجراء اختبار توازن حول ما إن كان من المفترض أن يكون هناك إفصاح أم لا. ودون الحصول على هذه المعلومات، فسوف يؤدي ذلك إلى تأخير العملية.

وبالطبع، يتلقى أمناء السجلات والسجلات شكاوى دون الحصول على اسم نطاق أو ما هو الحق القانوني الذي يحاول الطالب الادعاء به أو ما هي عناصر البيانات التي يريد الحصول عليها. وهذا ما يؤدي إلى تأخير العملية. إذن فأنتم بحاجة لشيء يكون مكتملاً لكي يتمكن أمين السجل أو السجل من التعاون واتخاذ قرار الإفصاح بشكل أسرع.

الشريحة التالية، رجاء.

ومن ثم فإنني أُجري استعراضًا لبعض المعلومات التي تمت مقارنتها للعرض الذي قمنا به، ألا وهي البيانات التي تم تقديمها طوعًا من جانب بعض أمناء السجلات والسجلات. وهي تمثل أمناء السجلات والسجلات الصغيرة والمتوسطة والكبرى والعديد من المناطق الجغرافية في العالم. ومن ثم كان هناك نطاق واسع من البيانات، فقد وصل بعض أمناء السجلات إلى 30 طلبًا وآخرون وصلوا إلى 3400 طلبًا. وكان للسجلات أقل من ذلك، وكانت الأرقام الأولية بعد قانون حماية البيانات العامة GDPR أعلى ولكنها ظلت إلى حد ما مستقرة عند هذا الحد منذ ذلك الحين.

إذن بعض النتائج الرئيسة تتمثل في أقل من 1% من النطاقات الإجمالية تحت الإدارة كانت معرضة للطلبات، وقد تنوعت بشيء ما استنادًا إلى نوع الإخفاء، حيث قانت مختلف الأطراف المتعاقدة بالتنفيذ والتقيد بالمواصفة المؤقتة وغيرها من الأشياء في ذلك.

كما أود تسليط الضوء على أنه بموجب نظام الوصول/الإفصاح القياسي، كانت هناك الكثير من المؤشرات المطلوبة من ICANN، وهو ما سيتم إبلاغ ICANN به أيضًا وبعد ذلك إبلاغ المجتمع به. ومن ثم سوف تكون لنا القدرة على تحقيق فهم أفضل، بمجرد

أن يكون هناك نظام للوصول/الإفصاح القياسي، وحول أنواع طلبات الإفصاح المقبلة، ومن الذي يقوم بها، وما هي النتائج، إلخ.

الشريحة التالية، رجاء.

وإليكم بعض النتائج التي توصلنا إليها. إذن بإمكانكم أن تروا من جانب السجلات حوالي نصف الوقت الذي قاموا فيه بالرفض أو الإخفاء، وأمناء السجلات، حوالي ثلثي الوقت قاموا بالرفض أو الإخفاء.

والإخفاء يعني أن السجل يقول من فضلكم اتصلوا بأمين السجل أو الرفض بسبب عدم وجود أساس قانوني. ويتم إجراء اختبار توازن.

بعض الأسباب الأخرى في ذلك في حين لم يتم الإفصاح عن أشياء بالضرورة هو النطاق المحمي من خلال خدمة خصوصية أو نطاق غير مسجل أو مع أمين السجل أو السجل ذلك.

الشريحة التالية، رجاء.

ما نوع البيانات التي تم تقديمها؟ وثلث الوقت كان بسبب بيانات المسجلين، وثلثي الوقت كان لمدير المسجل والبيانات الفنية. وبشكل عام، عندما لم يتم الإفصاح عن البيانات، كانت الممارسة القياسية متمثلة في توفير قدر من المسوغات والتفسيرات. وكما تعلمون، غالبًا عندما تكون هناك خدمة خصوصية/بروكسي وتقدم طلبات للإفصاح عن البيانات، فلا يكون هذا هو المسار المناسب للقيام بذلك. فخدمات الخصوصية/البروكسي لها مسارها والإجراءات الخاصة المعمول به لتنفيذ ذلك.

الشريحة التالية، رجاء.

إذن كان لبعض أمناء السجلات دعاوى استلموها بحالات رفض طلبات الإفصاح. أما السجلات فلم تقم بذلك. وأنتم ترون الأرقام بالنسبة لأمناء السجلات منخفضة للغاية. فغالبًا ما تأتي الطلبات من خلال التماس يأتي من آلية خاطئة وغالبًا ما يؤدي إلى عملية توعية

تثقيفية أو تفسير لسبب الرفض في تلك الحالة الخاصة. ومن الجدير بالذكر، لم تسقط أي من الالتماسات قرار الإفصاح أو عدم وجوده.

الشريحة التالية، رجاء.

إذن إليكم بعض المعلومات حول أنواع الطلبات التي تم تقديمها. وأنتم ترون حوالي ثلاثة أرباع هؤلاء كانوا من جهات إنفاذ القانون -- عفوًا، كانت طلبات ملكية فكرية، حوالي 15% من جهات إنفاذ القانون، والبقية كانت غيرهم، والتي تشتمل على باحثين في مجال الأمن، وطلب لا يخص النطاقات (يتعذر تمييز الصوت)، أو مرة أخرى، النطاقات التي لم تكن مع أمين سجل أو سجل.

الشريحة التالية، رجاء.

إذن من بين الطالبين الذين لدينا هنا، أرى واحدًا -- كان هناك طالب واحد لكل أربعة طلبات. فهناك إذن طالبين مكررين. وفي حقيقة الأمر، كان هناك طالب محدد هو مصدر نسبة 45% من الطلبات، وهي حصة كبيرة من كل حجم الطلبات الإجمالي.

ومن ثم أعتقد أن هذا -- شريحة أخرى، رجاءً.

كان هذا هو الوقت النموذجي للرد. وكان أقل من ثلاثة أيام على الإجمال. وكانت السجلات أسرع قليلاً من أمناء السجلات لأنه في الغالبي يكون السجل هو من يعيد توجيه الطالب إلى أمين السجل الذي يكون في موقع يؤهله إما لمعالجة البيانات أو اتخاذ قرار الإفصاح.

وهذا يأتني بنا إلى النهاية هنا. وأرجوا ألا أكون قد استفضت في الشرح بسرعة أكبر من اللازم. فقد أردت التأكد من توافر الوقت الكافي من أجل المناقشة بعد ذلك.

شكرًا.

جوناثان زوك: شكرًا لك، أوين. أعرف أن لديك الكثير من الأشياء التي تود استعراضها في فترة قصيرة. ولذلك أقدّر لك استعراض هذه المسألة سريعًا. هذه بيانات مفيدة للغاية.

أوين سميغلسكي: وأرجوا أن تلقوا نظرة على تلك الندوة النقاشية عبر الويب المنعقدة في سبتمبر/أيلول. فقد كانت ندوة على مدار ساعة ونصف ومن ثم تعيّن عليّ تلخيصها قليلاً. وقد كانت هناك مناقشة جيدة والكثير من المعلومات فيها أيضًا. شكرًا.

جوناثان زوك: هذا بالتأكيد. أرجوا من فريق العمل إلقاء نظرة على رابط التسجيل في برنامج زووم Zoom لهذا الأمر ونشره في مربع الدردشة، فسوف يكون هذا الأمر مفيدًا. وأعتقد أنها خلفية رائعة للغاية من أجل هذه المناقشات. وأنا أقدّر للأطراف المتعاقدة قيامهم بتجميع تلك البيانات.

وسوف نقوم بإعداد نسخة احتياطية من الشرائح، قليلاً أيها السادة فريق العمل، لأن مارك سفانكاريك قد انضم إلى الاجتماع ونريد أن نعطيه الفرصة لعرضها سريعًا بإيجاز.

إذن مارك، دون إضاعة المزيد من الوقت، تفضل بتناول الموضوع.

مارك سفانكاريك: شكرًا لكم جميعًا. هل يمكنكم سماعي؟

جوناثان زوك: نعم.

مارك سفانكاريك: أرجو المعذرة. الساعة المنبهة لا تعمل لدي. يا لها من ساعة هواة، أليس كذلك؟

مرحبًا، أنا مارك سفانكاريك من شركة مايكروسوفت، وأنا هنا لتقديم وجهة نظر حول نظرتنا للجريمة الإلكترونية في شركة مايكروسوفت وما يحدث بالنسبة لنظام WHOIS وقانون حماية البيانات العامة GDPR.

إذن سوف أحاول التزام السرعة بحيث يمكننا -- (ضحك) -- الحوار.

إذن سوف أضع شيئًا في مربع الدردشة. ألا وهو تقرير الدفاع الرقمي الجديد من شركة مايكروسوفت. وهذه هي المرة الأولى التي نقوم فيها بذلك. وهو شامل إلى حد ما، وهو يخبرنا على كيفية رؤيتنا للحالة الراهنة للجريمة الإلكترونية.

إذن هناك الكثير من النقاش حول ما إن كانت الجريمة الإلكترونية في تزايد أو انحسار مؤخرًا. وأنا غير متأكد من سبب -- السبب في أن يكون هذا الموضوع جدل دائر. فهو -- إنه في تصاعد. وجميع أنواع الجريمة الإلكترونية في تصاعد. ومن ثم ما يزال الدفاع ضدها أولوية أولى والكثير من الجهود تبذل في ذلك الإطار.

ومجموعة بيانات WHOIS واحدة من الأساليب التي نستخدمها من أجل معالجة جميع أشكال الجريمة، سواء كانت للشركات أو احتيال على المستهلكين، أو مكافحة القرصنة، أو تقييم لتهديدات الجهات الفاعلة في الدولة، وأكثر من ذلك بكثير.

أعتذر.

نعم، أنا لم -- أنا لم أقدم شرائح. عذرًا. وعندما قمت بعرض سريع للشرائح قبل الوقت، بدا وكأن ميلون وحده قد قدم أي منها. لذا اعتقدت أن الأمر سوف ينتهي إلى مناقشات فقط.

حسنًا-- عفوًا.

وعلى أية حال، فإن التحدي الذي نواجهه في مسألة WHOIS بموجب قانون حماية البيانات العامة GDPR حاليًا هو أننا لم نقوم بتطوير نظام يتيح لنا الوصول إلى البيانات إلى أقصى حد ممكن يمكن إتاحته بموجب الأنظمة والقوانين. وأعتقد أنه سوف يكون من الممتع النقاش حول ذلك أكثر في المجموعة، ولكن وصل الأمر إلى مرج الحصول على

قدر ما من المعلومات القانونية. وضمن المجموعة، لم يتحقق أي إجماع في الآراء حول ما هو المقصود فعليًا من التعليقات والآراء القانونية. وهذا فيما يخص الدقة والضرورة أشياء من هذا القبيل.

ومن ثم أعتقد أنه إذا كان لنا أن ننظر في تلك الندوة النقاشية من شهر سبتمبر/أيلول، وقضاء ما يقرب من 34 دقيقة في الإجراءات الفعلية المطروحة من أجل اختبارات التوازن، أعتقد أنكم سوف ترون أنها تختلف كثيرًا عن التعليقات والآراء التي وردت من شركة Bird & Bird فيما يخص ما تعنيه كلمة "ضروري". ومن ثم لدي بعض من هذه المعلومات هنا، إن أردتم إلقاء نظرة عليها -- أين هي؟ عذرًا. الروابط غير جاهزة الآن معي. أعتقد أنني قمت بذلك. وبشكل أساسي -- فإنني أعتذر. أعتذر حقًا أيها السادة.

سوف أضع هذه الأشياء في مربع الدردشة سريعًا. ولكن بشكل أساسي فإنها قادمة إلى -- وأنا سوف أدرج تعليقي هنا.

يمكننا الانتقال إلى موضوع آخر.

نعم يا عزيزي. نعم يا عزيزي. نعم يا عزيزي. وأثناء بحثي عن الرابط، فإن ما أريد قوله هو أننا سمعنا هذه الأشياء مثل وجود حلول للمنازعات، مثل الإجراءات الموحّدة لتسوية نزاعات أسماء النطاقات، ما يعني أنه لن يكون من القانوني الإفصاح عن البيانات بموجب نظام WHOIS، على سبيل المثال. وليس هذا هو الحال.

جوناثان زوك: مرحبًا، مارك. معكم جوناثان.

مارك سفانكاريك: لعلك تعلم، سأعود إليكم سريعًا.

جوناثان زوك: لستَ بحاجة لأن يكون معك روابط مباشرة. إذا كانت لديك أي نقاط هامة تريد طرحها، فأعتقد أن هذا هو المكان المناسب لذلك. ولكن يمكننا أيضًا -خلاف ذلك- مواصلة المناقشة.

مارك سفانكاريك: لنواصل المناقشة إذن. وسوف أعثر على هذه الروابط سريعًا جدًا.

لكن بيت القصيد هو أنه كان هناك الكثير من التأكيدات بأن نظام الوصول/الإفصاح القياسي لا يمكن تطويره إلا بطريقة فردية بسبب التعقيبات القانونية التي تلقيناها. وليس هذا هو الواقع. بل إن الواقع أننا قد حصلنا على خيارات إضافية، وقد اخترنا متابعة هذه القضايا.

كما أن المسار --

جوناثان زوك: شكرًا، مارك. أعتقد أن ما يجب علينا التركيز عليه فعيًا في هذا القرار ليس إعادة الإجراءات القانونية، ولكن النظر فعليًا في طبيعة هذه الطلبات، والتوقيتات التي كانت فيها، وهلم جرًا. وهذا هو السبب في أن بيانات أوين كانت مفيدة للغاية.

وأنا أعلم أن ديفيد تيلور قد قام بتجميع بعض البيانات حول جانب الطالب.

لكنني أعتقد أن ما نحاول الوصول إليه هو التسليم بأن قانون حماية البيانات العامة GDPR واقع، بالنظر إلى حقيقة أن -- حقيقة أن إنفاذه واقع، وتنفيذ توصيات عملية وضع السياسات المعجَّلة واقع، وقنوات الاتصال تعمل بين طالبي البيانات ومالكي البيانات، نظرًا للافتقار إلى مصطلح أفضل؟

أعتقد أن هذه هي المناقشة التي يجب أن نحاول إجراؤها، وكيف كان الحوار من أجل المضي قدمًا. وهذا هو السبب في أن بيانات أوين كانت مفيدة حقًا.

ولأنه وعلى سبيل المثال، أحد الأشياء التي طرأت مبكرًا في العرض التوضيحي هو الفكرة التي ذكرها غابرييل، وهو أنه بحلول الوقت الذي يتم فيه ملاحظة شيء ما -- عند ملاحظة احتيال بالتصيّد، يكون الأمر قد انتهي وهو ما يرجح عدم وجود الفترة الزمنية الكافية للأطراف المتعاقدة من أجل الرجوع إليك، بعد تقديم شكوى، على سبيل المثال.

ومن ثم أعتقد أننا نريد البدء في إجراء محادثة حقيقية حول ما هو واقعي من حيث ما قد يبدو عليه تبادل البيانات هذا.

إذن -- لنرى إذن. نعم، من بين المناقشات التي طرأت إلى حد ما هو أن بيانات الإبلاغ عن نشاط انتهاك النطاق DAAR تبدو وكأنها تقترح بأن انتهاك نظام أسماء النطاقات DNS على الإجمال قد تراجع. نعم، يبدو أن هناك بيانات أخرى قد ظهرت أو أنها سارت في طرق مختلفة، وهلم جرًا.

هل هناك من يريد تناول تلك الفكرة؟ وهذا موجه من لوك سوفير الذي طرح هذا السؤال في مربع الأسئلة. ما سبب وجود هذا الانقسام بين هذين -- المجموعتين المختلفتين من البيانات؟ لماذا لا تكون لدينا إجابة محددة حول ماهية الاتجاه الذي يسير فيه انتهاك نظام أسماء النطاقات DNS؟

غريغ آرون: مرحبًا، جوناثان. هذا غريغ. يمكنني الحديث حول هذا الموضوع لأنني قمت بتصميم وبناء نظام الإبلاغ عن نشاط انتهاك النطاق DAAR.

إذن ما يقوم به الإبلاغ عن نشاط انتهاك النطاق DAAR هو النظر في البيانات من واقع قوائم سواء قليلة ومختلفة تحتوي على أسماء نطاقات. وينظر في القوائم السوداء التي تحتوي على فئات من الظاهرة المسماة التصيّد والبرمجيات الضارة.

وما نتوقعه في المعتاد هو أنه في حالة مد وجزر على مدار الوقت. فإذا ما انحسر قليلاً لوقت ما، فقد يعلو مرة أخرى. وهذا هو المعتاد إلى حد ما.

ومن ثم فإنه يقوم بقياس بعض الأشياء النوعية للغاية من موارد محددة للغاية. ومن بين الأشياء التي نراها، رغم ذلك، أن أساليب المراوغة الجديدة قد تؤدي إلى انحسار عدد النطاقات التي ترونها. ولا ندري ما هو أثر توافر القليل من معلومات WHOIS، ما أثر ذلك على فاعلية الإدراج في القوائم السوداء. وعلى الرغم من أن بعض الموارد قد أجرت قياسًا لذلك وكانت هناك بعض المنشورات التي أوضحت أن من الصعب العثور على الأشرار، فإنك تحصل على نطاقات أقل في القوائم السوداء. وهذه واحدة من بين الآثار المحتملة.

ولا يعني هذا إذن أن مقدار الجريمة الإلكترونية قد تراجع. بل أنكم عثرتم على القليل من النطاقات وقد وجدتم القليل من النطاقات في القائمة التي تنظرون فيها.

وعندما يقول أوين أن إجمالي انتهاك أسماء النطاقات في انحسار، فقد لا يتعدى ذلك مقياس واحد طبقًا لملابسات محددة وموارد محددة.

ورغم ذلك وبصرف النظر عن طريقة القياس، فهي كثيرة. أما الأمر الآخر الذي يجب أن نذكر أنفسنا به فهو أن عدد أسماء النطاقات في أي قائمة محددة ليس مقياسًا للضرر الحادث أو ما تنطوي عليه من مخاطر. فمع انتهاك البريد الإلكتروني الخاص بالشركات على سبيل المثال، فإن حجم الأموال التي تُفقد في كل من عمليات الاحتيال هذه كانت في المتوسط في تصاعد. ومن ثم إذا كان لديك نفس عدد أسماء النطاقات، فإن الضرر الواقع على الضحايا يكون أكبر.

ومن ثم أعتقد أن يعتمد في حقيقة الأمر على ما نقوم بقياسه الآن. وهناك مؤشرات أخرى تقول بأن الرقم في تصاعد. ومن ثم فإن الإبلاغ عن نشاط انتهاك النطاق DAAR أحد الأشياء -- تقوم بشيء واحد وبطريقة خاصة. ولا أعتقد أن الأمر ربما يكون مؤشرًا على المنظومة الكاملة. شكرًا.

جوناثان زوك: شكرًا لك، غريغ. طرح ثيو غويرتس سؤالاً يقول فيه: ما مدى جودة البيانات عندما يقوم أمين السجل بالإفصاح عن البيانات؟ هل من الممكن استخدامها في عمليات التحري؟

لقد سمعنا من عدد من الأشخاص أن الأشخاص قد توارت بالفعل بسبب عدم توافر الدقة وخدمات الخصوصية والبروكسي، وما إلى ذلك. هل يمكنكم فعليًا -- أعتقد مثلما سأل ميلتون: هل يمكنكم فعليًا عزو الصعوبات التي تواجهونها إلى التغييرات التي طرأت نتيجة التوافق مع قانون حماية البيانات العامة GDPR؟ أعتقد أن هذا السؤال موجه إلى كل من العاملين في مجال أبحثا أمن الفضاء الإلكتروني وجهات إنفاذ القانون.

غابرييل أندروز: مرحبًا. أما غابرييل. أريد فقط التعليق على الموضوع وإضافة إجابة بسيطة على ذلك.

جوناثان زوك: تفضل.

غابرييل أندروز: أعتقد أن كفاءة الرد سوف تكون متفاوتة بشكل واضح، لكن من الجدير دائمًا الحصول عليها. والمرة الوحيدة فعليًا التي كان فيها الرد غير جدير بأي شيء هي إذا عائد من خدمة الخصوصية/البروكسي والتي لن تخبرك بأي شيء. حتى أننا رغم ذلك نجد أنه عندما يكذب المجرمون حول معلومات المسجلين الخاصة بهم أو كانوا قد استخدموا بيانات إثبات الهوية مخترقة من أجل السداد، وما إلى ذلك، فكل هذه تعد نقاط بيانات. ولا يمكن أبدًا معرفة ما هي نقطة البيانات التي سوف تكون فعليًا بمثابة الأساس في بدء تحقيقات. ومن ثم فإنني أفضل الحصول على بيانات مسجل احتيالية عن ألا أتمكن من الاطلاع على أي بيانات. وعلى الرغم من ذلك، وبشكل واضح، كلما كان مدى توثيق تلك البيانات أعلى عند التسجيل، كان ذلك أفضل بالنسبة لنا وأسوأ بالنسبة للمجرمين.

شكرًا لك، غابرييل.

طرحت ستيفاني بيرين سؤالاً: هل لدينا إحصائيات عن مدى ومقدار البيانات الصحيحة التي تجري سرقتها وتقديمها من أجل التعرف على بيانات المجرمين؟ فقد تمت إزالة البيانات التاريخية بالفعل. وما يزال هناك الكثير منها صالحًا.

غريغ آرون: هذا غريغ. يمكنني تناول هذه النقطة. مرحباً يا ستيفاني.

جوناثان زوك: رائع، شكرًا.

غريغ آرون: أعني، أنني قد نظرت في بيانات جهة الاتصال لملايين أسماء النطاقات المستخدمة في الانتهاكات على مدار سنوات. ما أراه هو أن المجرمين لا يميلون إلى سحب بيانات الآخرين واستخدامها. فهم يميلون إلى اصطناع بيانات فقط. والبعض منهم يقومون بعمل أفضل من غيرهم في هذا المجال. لكن من النادر نسبيًا من واقع خبرتي الشخصية رؤية بيانات مختلسة فحسب.

جوناثان زوك: حسنًا. شكرًا.

وأعتقد أنني سأسألك، هلا تفضلت بتشغيل الكاميرا عندما تتحدث أيضًا. فنحن نحاول التعرف على المزيد من الوجوه في هذه الاجتماعات عبر الإنترنت. لذلك عندما يكون -- عندما تجيب على سؤال ما، سيكون من الرائع لو تمكنت من تشغيل الكاميرا. وأنا أعلم أن هناك الكثير من عمليات النقر هنا وهناك، ولكن من المعتاد يمكن للناس رؤيتها.

قال فولكر: يبدو أن جريج يقول أنه لا فائدة من تعطيل أسماء النطاقات عند تلقي بلاغ عنها لأن الضرر قد حدث بالفعل. هذا يبدو غير بديهي.

غريغ آرون: لا. أعتقد أن فولكر لم يفهم جيدًا. من بين الأشياء التي رأيتها في الرسم البياني الذي عرضته هو، نعم، إذا قمت بتعطيل النطاق بالفعل، فستحصل على فائدة إضافية. أيضًا، يعد التصيّد الاحتيالي أحد أنواع الجرائم الإلكترونية الأقصر من حيث المدة. إذن فالمشكلات الأخرى تتمثل في أنك تحصل على فائدة أكبر بكثير عندما تقوم بتعليق اسم المجال الذي قام أحد المجرمين بتسجيله، لذلك فهو مفيد للغاية.

وعلى الرغم من ذلك، فالسؤال هو بالتأكيد؛ هناك فرق بين التخفيف والوقاية. ومن بين الأشياء التي رأيناها من واقع البيانات هو أن هناك أماكن معينة يذهب إليها المجرمون ويسجلون أسماء نطاقات. فيتم تعليق نطاقاتهم، وبعد ذلك كل ما عليهم فعله هو تسجيل المزيد منها. فنحن نعاني من مشكلة في النشاط التكراري. وسيكون من الأفضل لو أمكن التعرق على ذلك النشاط التكراري ومنعه مبكرًا.

ولعلكم تعمون، هل نفترض أن تعليق أسماء النطاقات لا يجدي أي نفع، لا، بل هو إجراء جدير بالتنفيذ.

أؤكد مرة أخرى، أن الهدف الرئيسي هو حماية الأفراد المعرضين للوقوع ضحايا لتلك الأعمال.

ميلتون مولر: هل يمكنني المشاركة، جون؟

جوناثان زوك: بالتأكيد، ميلتون. تفضل.

ميلتون مولر: مرة أخرى، أعتقد أننا نحتاج حقًا إلى التركيز على عملية إخفاء البيانات ما قبل WHOIS وبعدها. وهذا هو الهدف هنا. ولا أعتقد أن هذا الأمر مرتبط كليًا بالقول بأن التصيّد والاحتيال يمثل مشكلة. ونحن جميعًا على علم بذلك.

والسؤال الذي يطرح نفسه هو: هل كانت المعركة ضد التصيد الاحتيالي أو غيره من أشكال الجرائم الإلكترونية، وما مقدار الاعتماد الفعلي على الوصول المفتوح إلى بيانات WHOIS؟

وأعتقد أن المجرمين قد توصلوا إلى طرق قوية إلى حد ما في تجنب الاكتشاف وأن معظم الكوابح الحقيقية التي يتم وضعها أمام النطاقات المستخدمة في التصيّد تأتي من عمليات التعليق والإيقاف ومن الخوارزميات التي تعمل على كشف الأنماط وحظرها سريعًا وحسب. وليس من الواضح بالنسبة لي ما إن كان لوجود أو عدم وجود بيانات WHOIS علاقة بذلك. وهناك -- مرة أخرى، بالنظر إلى البيانات، لا نرى أي ارتباط إحصائي بين مشاكل ما قبل WHOIS وما بعدها. لذا اسمحوا لنا أن نركز على ذلك.

لا أعتقد أنه يمكنكم ببساطة القول بأننا كنا راضين عن ذلك عندما كان لدينا هذا الوصول. ولكن عندما كان لديكم هذا الوصول إلى البيانات، كان التصيّد العشوائي والمفتوح لا يزال يمثل مشكلة. بل كان يمثل مشكلة متنامية للغاية وتزداد بمعدل أسرع مما هو عليه الآن.

لذا اسمحوا لنا أن نركز على السبب والنتيجة، إن أمكننا ذلك.

جوناثان زوك: سؤال رائع، ميلتون. هل هناك من يريد تناول ذلك السؤال من منظور جهات إنفاذ القانون أو منظور أمن الفضاء الإلكتروني؟

غابرييل أندروز: حسنًا، يمكنني إضافة تعليق مفاده أن التحقيقات تتأثر سلبًا بعدم توافر تلك البيانات. وثمة طرق عديدة لحدوث ذلك، ولكن ربما يستلزم إجراء حوار أكبر.

أردت أن أنبه هذه اللجنة إلى تعليقاتي السابقة بأن واجباتنا لا تشتمل فقط على جانب إرجاع الأسباب، ولكن أيضًا يشتمل أيضًا في بعض الأحيان الإخطار السريع للضحايا المحتملين. وهذا مثال من العالم الواقعي حيث نكون غير قادرين على فعل شيء تمامًا وأننا نستخدم

ليس فيه المعرّفات الخاصة بأصحاب البيانات ضمن نظام أسماء النطاقات ولكن المعرّفات المرتبطة بالضحايا التي يجري استهدافها دومًا. لذلك ثمة افتراض بأنها بيانات صحيحة. ولكن إذا لم تتم إتاحتها بسرعة، فإن المحادثات المهمة التي يمكن أن تحدث عبر الهاتف لشخص ما حسابات بريده الإلكتروني قد تكون مخترقة ويكون مستهدفًا في ذلك الوقت أو في ذلك اليوم أو في اليوم التالي، فهي تمكننا من الحصول على تلك المحادثات. ولم تعذر علينا ذلك، ولا يمكننا تفادي الضرر لكل المواطنين في جميع أنحاء العالم.

جوناثان زوك: غابرييل، هل تقترح أن استخدام البيانات سيكون أكثر قيمة في الوصول إلى الأبرياء أكثر من تعقب المجرمين؟

غابرييل أندروز: لا أعتقد أنه يمكنني إجراء تقييم. يمكنني القول بأنني أعلم أنها تستخدم لكلا الغرضين، إن أنصفنا القول. وأنا لا -- وأنا أواجه صعوبة في تقديم ادعاءات وساعة وكاسحة حول ما يحدث في الغالب لأنني ببساطة قد حاولت جمع البيانات وقد رأيتُ مدى صعوبة حمل المحققين على قضاء وقت خلال أعمالهم المكتظة كي يقدموا لنا تقارير وبلاغات عن ذلك. فقد حاولت قرابة 82 مرة أن أحصل على معلومات حول المسجل ونجحت في 42 محاولة منها. اتفقنا؟ وهي لا تتعقب حالات الفشل. فمن الصعب جدًا إذن أن نعود مرة أخرى ونقدم بعض الحقائق التي أعرف أنها ستكون مفيدة للغاية هنا.

لكن ما يمكنني قوله هو أنني عندما كنت أجمع حكايات هذه الحالات، كانت تلك الحكاية هي التي حصلت عليها وكان أكثر ما أذهلني هو الإحباط الذي شعر به بعض المحققين الذين كانوا يحاولون فعل الشيء المناسب، ألا وهو تقديم الإخطارات للأشخاص الذين سيتعرضون للأذى ووجدوا أنهم مكبلي الأيدي. وهذا لا يعني أنهم لا يستطيعون بطريقة ما، أنه ربما بطريقة ما يمكنهم استكشاف سبل أخرى.

هذا يعني فقط أن هذه هي الطريقة الأسرع المستخدمة للعمل معهم وهي غير مجدية. وليس هذا إلا شيء أردت تسليط الضوء عليه.

وسأترككم تواصلون نقاشه.

جوناثان زوك: شكرًا. غابرييل.

أوين، أعلم أن جزءًا من العرض التقديمي الذي قدماه الأطراف المتعاقدة مؤخرًا حول الوصول إلى البيانات قد أرسي بعض أفضل الأسس المستخدمة في تنسيق الطلبات للإسراع بتنفيذها، وما إلى ذلك. هل هناك أي أمثلة أو أي بيانات مرتبطة بطالبي البيانات الذين يقومون بذلك بتلك الطريقة؟

وهل هناك علاقة إذن بزيادة احتمالية تقديم البيانات بطريقة أسرع؟

أوين سميغلسكي: شكرًا لك، جوناثان. أنا أوين سميغلسكي للعلم والإحاطة. لا يمكنني حقاً استخلاص أي استنتاجات من ذلك. لقد كانت بالتأكيد مجموعة بيانات محدودة وليست بالضرورة مجموعة بيانات شاملة، لكن تجربة الأطراف المتعاقدة تمت عندما كانت لديهم طلبات بمعلومات إضافية، وكانت اهم القدرة على معالجتها بشكل أسرع. وكانت لهم القدرة على إجراء اختبارات التوازن الصحيح بشكل أسرع. ولكن لمجرد أنك قدمت كل المعلومات لا يعني أنها ستجتاز هذا الاختبار الخاص بالتوازن. فهل هناك وسائل أقل تدخلاً لمتابعة ذلك بدلاً من مجرد الحصول على البيانات. وهذا الأمر يضم عددًا من الأسئلة والعوامل التي يمكن أن تنطبق.

ولا يلزم بالضرورة أن يؤدي ذلك إلى الإسراع بالعملية. بحيث يمكن أن تصل بك إلى نتيجة في هذا الأمر. حيث أظهرت غالبية البيانات أن غالبية الطلبات مقدمة من أجل انتهاك العلامات التجارية. وبالتالي، فهذه ليست بالضرورة واحدة من تلك الحالات العاجلة

التي تحتاج إلى إزالة شبكة بوت نت. فهناك مسارات أخرى يمكن اللجوء إليها، مثل الإجراءات الموحّدة لتسوية نزاعات أسماء النطاقات أو التعليق السريع الموحد أو شيء مماثل لا تحتاج لبيانات من أجل القيام به. لذلك هذا أقل تدخلاً وهو ما يمكن أن يجتاز بذلك -- سيفشل في اختبار التوازن هذا لأن هناك وسائل أقل تدخلاً للقيام بذلك.

جوناثان زوك: أوين، هل تعتقد أن اختبار الموازنة سيظل أساسًا للتعامل مع حالة على حدة أم ستكون هناك طريقة ما، على سبيل المثال، الأشخاص الذين قاموا بتسجيل الدخول إلى إطار عمل انتهاك نظام أسماء النطاقات DNS للالتقاء والتوصل إلى سلسلة ما من القرارات التي تجعلها أقل قليلاً من يكون صندوق أسودًا للأشخاص الذين يحاولون الحصول على البيانات من الأطراف المتعاقدة؟

أوين سميغلسكي: شكرًا لك، جوناثان. أنا أوين مرة أخرى للعلم والإحاطة.

لا أستطيع حقًا أن أقول ما الذي سيحدث في المستقبل. فما يزال هناك الكثير من الغموض وعدم اليقين بشأن ما لن يتم السماح به. بعض الإرشادات في ذلك هو أنه بالفعل، لا، فلا يمكن بالضرورة أتمتة بعض الأشياء. وهناك الكثير من الأمور المجهولة في طلبات الإفصاح عن البيانات.

وأنا أعلم أنني رأيت بعض المحادثات هناك تقول، حسنًا، الكونغرس الأمريكي سوف -- يجب أن يمرر شيئًا لجعل نظام WHOIS متاحًا للجمهور. ولكن بالنسبة لأمين سجل كبير مثل Namecheap يضم ملايين العملاء في جميع أنحاء العالم، ليس من الممكن - بالضرورة- القول بيقين بنسبة 100 في المائة أن هذا الشخص موجود خارج نطاق سلطة قضائية ما، وهذا ليس خاضعًا لشيء يتعلق بخصوصية البيانات، والإفصاح عن هذه البيانات من شأنه أن يعرضنا للمساءلة المدنية والجنائية المحتملة. لذلك فهو ليس شيئًا يمكنك بسهولة وضع أسلوب يناسب جميع الأحكام في هذا الصدد. قد يكون بعض أمناء أصغر أو أنه مرتكزون فقط في منطقة معينة أو أن لديهم نوع مختلف من نماذج الأعمال.

لذلك أعتقد أنه مع تطور هذا الأمر بمرور الوقت، وهو بالتأكيد مضمّن في اللجنة الاستشارية للأمن والاستقرار من أجل تطويره وتغييره عن طريق عملية السياسة، أعتقد أنه سيتطور بالتأكيد، ولكن من السابق لأوانه التنبؤ بكيفية حدوث ذلك.

شكرًا.

جوناثان زوك: شكرًا لك، أوين. أظن أن لوري شولمان قد تساءلت بشأن نفس المشكلة، عما إذا كنت ترغب في مناقشة تجربة Namecheap النوعية أم لا من حيث عدد الطلبات التي تم تلقيها وعدد الطلبات التي أدت إلى الإفصاح عن البيانات.

أوين سميغلسكي: مرحبًا، جوناثان. أنا أوين مرة أخرى. ليس هذا شيء يمكنني مناقشته هنا. فأنا لا أستطيع الدخول إلى تلك البيانات حاليًا.

جوناثان زوك: رائع. شكرًا.

لذا -- أعلم أنه كانت هناك محادثة، فقد كنت أحاول مشاهدة كل الأسئلة في المربع والدردشة لمحاولة اكتشاف ما يقوله المجتمع ككل. وأعلم أن مايك غراهام، إذا كنت معنا، أنك طرحت سؤالاً محددًا حول تغيير نوعي حدث مع عملية إخفاء البيانات. هل هذا شيء ترغب في تشغيل ميكروفونك ومشاركته معنا؟ لأننا قد تجاوزناه في الدردشة.

وأنا لا أقصد إحراجك في هذا الأمر.

نعم، هل يمكنك تشغيل الميكروفون الخاص بك أو هلا تفضل فريق العمل بالسماح لمايك بتشغيل ميكروفونه؟

مايكل غراهام: هل الصوت بعمل الآن؟

جوناثان زوك: نعم، إنهم كذلك. شكرًا.

مايكل غراهام: أعتذر عن ذلك. حقًا، لا يمكنني الإفصاح إلا عن القليل من المعلومات، وذلك من حيث الجهد والتكلفة. وهناك طريقتان مختلفتان كان لهما تأثير. تتمثل أحداهما في مجرد اكتشاف المعلومات حتى نتمكن من تحديد ما إذا كان اسم نطاق معين قد تم تسجيله عن طريق الاحتيال وأنه يتم استخدامه أو ربما تم تسجيله من قبل شخص له علاقة بشركتنا وهو ببساطة أنه القرصنة بالأخطاء الإملائية عن غير قصد.

وبالتأكيد في الحالة الأخيرة ، نتفهم أن هناك الكثير من الأشخاص الذين يدخلون الإنترنت، وليسوا محنكين وقد يفعلون شيئًا -لعلكم تعلمون- قد يضر ليس فقط بقدرتنا على الوصول إلى المستهلكين وقدرتهم (يتعذر تمييز الصوت) للقيام بذلك ولكي تكون مواطنًا صالحًا على الإنترنت، ولكن فيما يتعلق بالبحث فقط والتكلفة التي تتحملها الشركات، فإن هذه تكلفة هائلة وتمثل نفقات إضافية لمعرفة تلك المعلومات. وفيما يتعلق بالإساءة الحقيقية -- وهذه الإساءة ليس بالضرورة تصيّدًا ولكن في بعض الحالات في التصيّد بالنسبة لنا وفي حالات أخرى فقط الخروج والتزوير الذي يحدث على الإنترنت. لقد ارتفعت كلفة التحقيق ارتفاعًا كبيرًا. وفي مرحلة ما، لسنا وحدنًا من يتحمل هذه التكلفة، بل يتحملها المستهلكون أيضًا، سواء من الناحية المالية أو من حيث قدرتهم على الوثوق بما يجدونه على الإنترنت. وهذا شيء يثير قلقنا حقًا، أي أن تكون لهم القدرة على العثور على ما يبحثون عنه وعدم التعرض للوقوع في أحد هذه المخططات التي يبدو أنها مستمرة بشكل يومي.

جوناثان زوك: شكرًا لك، مايكل.

تعتبر قضية التكلفة قضية معقدة، لأن من الواضح أن أولئك الموجودين في مجتمع طالب البيانات ليسوا دائمًا حساسين للتكاليف التي يتم فرضها على الأطراف المتعاقدة أيضًا. ولعلكم تعلمون أن هذا من أجل تنفيذ بعض الأمور المطلوبة منهم.

لذا، إذا كانت مجرد تكلفة ممارسة الأعمال من أجل الامتثال للقانون، فأعتقد أن هذا -- ستكون مسألة توزان معقدة أيضًا.

إليزابيث --

ميلتون مولر: هل يسعني التعليق على هذا؟

جوناثان زوك: نعم، ميلتون. تفضل.

ميلتون مولر: التكلفة هي في الحقيقة ما يدور حوله كل هذا لأنه ولمدة 20 عامًا، لم يحصل مقدمو الطلبات على وجبة غداء مجانية فحسب، بل تم دعمهم ماديًا بشكل أساسي من قبل نظام ICANN. لذلك نحن نعرض بشكل أساسي على مسجلي أسماء النطاقات عقد التزام ينص على أنك تريد اسم نطاق، وأنك ملتزم -دون موافقة منك ودون أي رأي في الموضوع- بجعل البيانات المحددة لهوية أصحابها الخاصة بك في متناول الجميع ومتناول أي شخص يريدها. وقد أدى ذلك إلى فرض تكاليف على المسجلين، ما أدى إلى دعم وصول الأشخاص، حيث كان البعض منهم يقوم بجمع هذه المعلومات وبيعها وجني الأموال منها.

وأعتقد أن -- ما فعلناه هو، مع نظام الوصول/الإفصاح القياسي هو أننا قلنا، حسنًا، ستتم موازنة التكاليف بطريقة أكثر عدلاً وفعالية. فإذا كنت طالبًا كبيرًا، ويمكننا جميعًا التفكير في شركتين تقومان باستخراج غالبية الطلبات، أعتقد أن بيانات أوين كانت مفيدة جدًا في

الواقع حول ذلك -كما تعلمون- فأنت الشخص الذي يتسبب في التكلفة على النظام. أنت مسبب التكلفة، إذا جاز التعبير، وعليك أن تدفع أكثر. يجب عليك دعم النظام إما من خلال الرسوم المستخرجة من المستخدم أو نوع ما من رسوم الاعتماد المتدرجة التي من شأنها أن تغطي تكلفة إتاحة هذه البيانات.

وإذا كان لهذه البيانات أن تكون متاحة بالسرعة التي يريدها بعض الأشخاص، فمن الواضح أنك تفرض تكاليف باهظة على الطرف المتعاقد الذي يتوجب أن يكون لديه شخص يجلس حوله يقوم بتقييم هذه الطلبات. ومرة أخرى، يمكنك تجنب بعض هذه التكاليف عن طريق الأتمتة، ولكن الأتمتة يمكن أن تكون أيضًا غير قانونية إذا كانت لا تقوم بالفعل بإجراء النوع المناسب من الفحص على طبيعة وماهية الطلب المقدم.

لذلك، وكما قلتُ جوناثان، فإنه يمثل تحديًا معقدًا، وأعتقد أن هذا -- من حيث أهداف هذه اللجنة، أعتقد أنه سيكون من الجيد أن يكون لديك وعي أكبر بالطريقة التي يتم بها توزيع التكاليف بطريقة متوازنة عبر مختلف مجموعات أصحاب المصلحة.

جوناثان زوك: شكرًا لك، ميلتون.

ناتالي ليوري تسأل: تقدم معظم السجلات الأوروبية خدمة إصدار بيانات متوافقة مع قانون حماية البيانات العامة GDPR إذا كان بإمكان مقدم الطلب تقديم دليل على تسجيل علامة تجارية ما. هل من المعروف ما إذا كانت نطاقات gTLD أو نطاقات ccTLD الأخرى تفكر في تبني نموذج مماثل؟ فهذا يساعد جهود الإنفاذ بشكل كبير.

أوين، قد تكون أنت الشخص الوحيد القادر على الرد على هذا السؤال، حتى لو كنتَ لا تعرف الإجابة.

أوين سميغلسكي: أعتذر. لقد كنت أحاول متابعة الدردشة هنا. أي سؤال كان ذلك؟

جوناثان زوك: أعتذر لكِ، ناتالي ليروي. إنه في أسفل السؤال - أسفل مربع الأسئلة.

أوين سميغلسكي: لا أعرف إذن -- شكرًا. أنا أوين للعلم والإحاطة.

لست متأكدًا مما إذا كان هناك نطاقات gTLD أو نطاقات ccTLD أخرى تتبنى نماذج مماثلة، ولكن كما تعلمون وأؤكد لكم مرة أخرى، مع تقدم هذا الأمر في نظام الوصول/الإفصاح القياسي هذا، قد يكون هناك بعيدًا عن المستخدمين الذين هم بصدد الحصول على نطاق gTLD معين أو شيء من هذا القبيل.

مرة أخرى، كان تقرير المرحلة الثانية لعملية وضع السياسات المعجَّلة هو نقطة البداية. فقد كنا واقعين تحت ضغوط من حيث الوقت لإنجاز كل شيء، ولوضع كل شيء هناك. كمت كان هناك الكثير من المشاركين في الداخل والخارج ممن أرادوا القيام بشيء أسرع مما كنا نفعله، ولذا بذلنا قصارى جهدنا في ظل ضيق الوقت المتاح أمامنا.

لذلك أعتقد أن هذا يمكن أن يمثل بالتأكيد اقتراحًا للمضي قدمًا مع تطور نموذج نظام الوصول/الإفصاح القياسي لوضع شيء ما هناك. أعتقد أنه إذا كان هذا أمرًا متفقًا عليه وملتزم بالقوانين، فمن المؤكد أن ذلك قد يجعل (يتعذر تمييز الصوت) أسهل.

شكرًا.

جوناثان زوك: شكرًا لك، أوين.

أرجو أن يكون هذا مفيدًا، ناتالي. أعتقد أن هذا سؤال أكبر بكثير مما سنكتشفه اليوم.

وقد طلبت لورين الرد على ميلتون. إذن تفضلي رجاءً، لورين. أو، هلا تفضل فريق العمل بتفعيل ميكروفون لورين.

لورين كابين: أعتقد أن ميكروفوني يعمل بالفعل.

جوناثان زوك: حسنًا، رائع.

لورين كابين: شكرًا. وأردت أن أعبر عن اتفاقي مع بعض النقاط التي أوضحها ميلتون حول اعتبار هذه المعلومات سلاحًا ذا حدين. وبالتأكيد من الممكن استخدمها في أغراض ضارة. وبالفعل، ميلون، فإننا نرى ذلك أيضًا في بيانات الشكاوى.

ولكن من ناحية أخرى، فإن نظام أسماء النطاقات يعد موردًا عامًا. وقد ضرب ميلتون مثلاً بالأشياء التي يتم سحبها واستخدامها لأغراض خبيثة وهذا مخالف للقانون، ولا يوجد خلاف بشأنها.

لكن قانون حماية البيانات العامة GDPR لا يحمي بيانات الشخصيات الاعتبارية. وأنا أتطلع إلى جهود تطوير السياسة المستمرة في هذا الصدد، لأن الجمهور لديه الحق في معرفة معلومات الشخصيات الاعتبارية. ومن خلال هذا التغيير بالسماح للمستخدمين بمعرفة من يقف وراء النطاقات التي ليست كيانات فردية، فإن ذلك من شأنه أن يقطع شوطًا طويلاً في مساعدة الجمهور وإنفاذ القانون في تحقيقاتهم وجهود العناية الواجبة.

ولعلكم تعلمون، بما أننا نطلب تقديم معلومات معينة لاستخدام الموارد العامة ، سواء كانت رخصة قيادة أو رخصة تجارية وبعض هذه المعلومات متاحة للجمهور، يجب أن يتم ذلك من أجل المعلومات القانونية المرتبطة بالشخصيات الاعتبارية.

جوناثان زوك: شكرًا لورين.

هناك المزيد من الأسئلة، وبالتالي سيقوم فريق العمل بجمعها، وسنحاول إيجاد طريقة لكتابة الإجابات. لسوء الحظ، نفد وقتنا. لقد كان حوار جيد. ومن الصعب دائمًا إبقائه مرتكزًا على موضوع محدد. وأيضًا- لكن للإجابة على السؤال المقدم من جيف حول الغرض من الجلسة العامة، فأنا لست متأكدًا. ولكن من الناحية المثالية، كلما فهمنا ماهية الموقف الواقعي قبل التغيير وبعده في سياسة ICANN، كنا أكثر استنارة حيال الخطوات التي يجب اتخاذها بعد ذلك. وأعتقد أن الغرض من هذه المناقشة، كان - إلى أقصى حد ممكن- متمثلاً في اكتساب فهم لما نتج عنه هذا التغيير في الوضع الراهن من حيث تدفق البيانات وتوافر المعلومات اللازمة لحماية المستهلك في أبحاث أمن الفضاء الإلكتروني.

لذا نأمل أن تكون هذه مهمة لتقصي الحقائق بشيء ما. ومن الواضح أن هناك الكثير من أعمال البحث الحقائق يجب القيام بها. هناك الكثير من الأسئلة المتبقية في مربع الأسئلة. وسنرى ما في وسعنا لمعالجتها، لكن وقتنا اليوم قد نفد. الساعة الآن 3:00 صباحًا بالنسبة لي، لذلك ربما نفد ما لدي من أشياء ذكية يمكن قولها، لذا سأقول شكرًا لجميع المتحدثين وجميع من حضروا لمناقشة هذا الأمر. سنلقي نظرة على الدردشة، وما إلى ذلك، ونستخدمها وقودًا لنا في المحادثات المقبلة.

شكرًا جزيلاً للجميع على هذا. انتهى هذا الاجتماع.

[نهاية النص]