TLP:CLEAR

مشروع مدونة قواعد الأخلاق والسلوك المهني لدى منتدى أفرقة الأمن والتصدي للحوادث (FIRST)

يمكن لأعضاء أفرقة الأمن والتصدي للحوادث (الأفرقة) النفاذ إلى العديد من الأنظمة الرقمية ومصادر المعلومات. وإجراءاتهم يمكن أن تغير العالم. وكعضو في هذه المهنة، يجب أن يدرك عضو الفريق المسؤولية تجاه الجهات التي يخدمها وغيرها من المهنيين الأمنيين، وكذلك تجاه المجتمع الأوسع. ويجب على الفرد أيضاً أن يدرك مسؤوليته تجاه حسن حاله.

وقد وُضعت مدونة القواعد هذه لإلهام وتوجيه السلوك الأخلاقي لجميع أعضاء الفريق، بمن في ذلك المزاولون الحاليون والمحتملون، والمدرسون، والطلاب، والجهات المؤثرة، وأي شخص يستخدم تكنولوجيا الحوسبة بطريقة ذات أثر. وتتضمن مدونة القواعد مبادئ صيغت على أنها بيانات المسؤولية، من منطلق أن المصلحة العامة هي دائما الاعتبار الأساسي. ويُتمّم كل مبدأ بمبادئ توجيهية تقدم تفسيرات لمساعدة محترفي الحوسبة في فهم المبدأ وتطبيقه.

ويعرَّف بالواجبات أدناه، ولكنها ليست مرتبة حسب تسلسل الأهمية. وينبغي ألا يُنظر إلى هذه الواجبات على أنها متطلبات مطلقة، بل على النحو المذكور في المرجع IETF RFC2119 لتعريف "**ينبغي**":

> "قد توجد أسباب وجيهة في ظروف معيَّنة لتجاهل بند معيّن، ولكن يجب أن تُفهم كل التداعيات وأن تُدرس بحرص قبل اختيار مسار آخر".

وللاطلاع على معلومات أوفى عن كيفية التعامل مع المعضلات الممكنة، انظر التذييل A.

واجب الجدارة بالثقة

الثقة هي أساس العديد من العلاقات بين الأفرقة، وكثيراً ما تكون مطلوبة قبل أن يتسنى تبادل ذو مغزى للمعلومات. وقد بُني مجتمع منتدى أفرقة الأمن والتصدي للحوادث (FIRST) على هذه الثقة، ولا يمكنه الاستمرار في العمل بهذه الطريقة إلا بوجود مستوى معقول من الثقة بين الأفرقة.

والجدارة بالثقة تعني أن أعضاء الفريق ينبغي لهم الاقتصار على: 1) الدخول في التزامات يمكنهم الإيفاء بها، 2) التصرف بشكل تعرف الأفرقة الأخرى عقباه (من قبيل احترام معيار TLP)، 3) إعلاء علاقة الثقة التي تربطهم بالأفرقة الأخرى. وينبغي أن تُفترض علاقة الثقة في البداية وأن تكون متعدية، أي الثقة عند الاستخدام الأول (TOFU)، وأن تعزز ثقة الأفرقة التي تثق بها أفرقة أخرى.

واجب الكشف المنسق عن ثغرة

ينبغي أن يعمد أعضاء الفريق الذين يحاطون علماً بثغرة أمنية إلى الكشف المنسق عن الثغرة من خلال التعاون مع أصحاب المصلحة لسد الثغرة الأمنية وتقليل الضرر المرتبط بالكشف إلى أدنى حد. ومن بين أصحاب المصلحة، على سبيل المثال لا الحصر، المبلِّغ عن الثغرة، والبائع المتأثر (الباعة المتأثرون)، والمنسقون، والمدافعون، والعملاء والشركاء والمستخدمون في اتجاه مقصد سلسلة التوريد.

وينبغي لأعضاء الفريق التنسيق مع أصحاب المصلحة المناسبين للاتفاق على جداول زمنية وتوقعات واضحة لنشر المعلومات، وتقديم تفاصيل كافية للسماح للمستخدمين بتقييم مخاطرهم واتخاذ تدابير دفاعية قابلة للتنفيذ.

واجب الكتمان

على أعضاء الفريق واجب الاعتصام بالكتمان عند الاقتضاء. ويمكن التقدم بطلبات صريحة لإبقاء بعض المعلومات طي الكتمان، بواسطة بروتوكول إشارات المرور (TLP) على سبيل المثال. وينبغي لأعضاء الفريق احترام هذه الطلبات كلما أمكن ذلك. وإذا تعذر إبقاء المعلومات طي الكتمان، بسبب تعارض مثلاً مع متطلبات القوانين المحلية أو العقود أو واجب الإبلاغ، ينبغي لعضو الفريق إبلاغ مالك المعلومات بهذا التعارض على الفور.

وتستند بعض واجبات الكتمان إلى القوانين أو اللوائح أو العادات. فإذا كانت بعض الأطراف، أثناء التصدي لحادث، ملزمة بالكتمان أو كانت تتوقعه بناءً على هذه الاعتبارات، ينبغي لها بذل قصارى جهدها لتوضيح هذه التوقعات مقدماً. وعندئذ ينبغي لجميع الأطراف الالتزام بالتوقع المذكور أعلاه الذي يؤكد طلبات صريحة لإبقاء المعلومات طي الكتمان عندما يكون ذلك ممكناً.

واجب الإشعار بالاستلام

تتلقى الأفرقة معلومات من العديد من المصادر المختلفة: من الباحثين والعملاء والأفرقة الأخرى، والهيئات الحكومية، ومَن إلى ذلك. وينبغي لأعضاء الفريق الرد على الاستفسارات في الوقت المناسب، حتى لو كان ذلك لمجرد تأكيد استلام الطلب. وينبغي لأعضاء الفريق تهيئة التوقعات بشأن المستجدات التالية عندما يكون ذلك ممكناً.

واجب الإجازة

لأعضاء الفريق حاجة مشروعة وحق في أن يفهموا مجالات مسؤولياتهم، وأن يقتصر عملهم على الأنظمة التي يجاز لهم النفاذ إليها. ويتعين أن يكون أعضاء الفريق على دراية بكيفية تأثير إجراءاتهم على الجهات التي يخدمونها، وأن يحرصوا على عدم التسبب في ضرر إضافي أثناء أداء واجباتهم. وينبغي توضيح ما يمكن أن يظهر من ذيول هذه الإجراءات لأصحاب المصلحة المتضررين. وحيثما أمكن، ينبغي التشاور مع الجهات التي يخدمونها قبل إجراء التغييرات على أنظمتها.

واجب الإبلاغ

ينبغي أن يعتبر أعضاء الفريق أن من واجبهم إبقاء الجهات التي يخدمونها على علم بالتهديدات والمخاطر الأمنية الماثلة. وعندما ترد إلى أعضاء الفريق معلومات يمكن أن تؤثر سلباً على السلامة والأمن أو أن تحسنهما، فمن واجبهم إبلاغ الأطراف ذات الصلة أو جهات أخرى يمكنها المساعدة، بالجهود المناسبة، مع مراعاة الكتمان، وقوانين ولوائح الخصوصيات، أو الالتزامات الأخرى حسب الأصول.

واجب احترام حقوق الإنسان

ينبغي أن يدرك أعضاء الفريق أن إجراءاتهم يمكن أن تؤثر على حقوق الإنسان للآخرين، من خلال تبادل المعلومات، أو التحيز الممكن في إجراءاتهم، أو من خلال انتهاك حقوق الملكية. ويمكن لأعضاء الفريق النفاذ إلى مجموعة واسعة من المعلومات الشخصية والحساسة والمكتومة أثناء التعامل مع الحوادث. وينبغي التعامل مع هذه المعلومات بطريقة تعلي من شأن حقوق الإنسان.

أثناء التعامل مع الحوادث، ينبغي للمستجيبين ألا يتصرفوا بطريقة متحيزة وينبغي أن يبذلوا قصارى جهدهم لإزالة التحيز من عملياتهم وصنع قرارتهم، على أن يتولى المستجيبون هذه الإزالة أو أن تُدمج في الخوارزميات.

ولأغراض هذا المبدأ، يشمل مفهوم "الملكية" (وفق إعلان الأمم المتحدة لحقوق الإنسان: المادة 17) الأشياء غير الملموسة مثل الملكية الفكرية بالإضافة إلى الأفكار والمفاهيم بوجه عام، بغض النظر عما إذا كانت محمية قانوناً (ببراءة اختراع على سبيل المثال).

واجب تجاه صحة الفريق

تتحمل الأفرقة مسؤولية التمكن من الاستمرار في تقديم الخدمات التي وعدت بتقديمها إلى الجهات التي تخدمها. وتشمل هذه المسؤولية الصحة الجسدية والعاطفية للفريق.

ولاحترام الأعضاء الذين يشكلون فريقاً واحداً كأشخاص وكذلك لتمكين الديمومة الحيوية لمستوى كاف من الخدمة على المدى الطويل، ينبغي أن يسعى الفريق للحفاظ على بيئة عمل صحية وآمنة وإيجابية تدعم صحة (جميع) أعضائها من الناحية الجسدية والعاطفية. وللتصدي لأزمة، ينبغي أن تدعم العمليات "الطبيعية" الصحة العاطفية وتقليل التوتر.

واجب تجاه قدرة الفريق

تشكل إدارة الحوادث موضوعاً آخذاً في التطور ينبغي لأعضاء الفريق دراسته باستمرار. وينبغي أن يقدم الفريق الموارد لأعضائه ليتمكنوا من دراسة وتطبيق وتطوير المعارف التكنولوجية والعلمية في مجال (مجالات) مسؤولية ما. ويمكن أن تساهم في ذلك ساعات التحصيل التدريبي أو التعليمي CPE/CEU، ولكنها مجرد تمارين على الالتزام ولا تكفي للإيفاء بهذا الواجب. وينبغي أن يحافظ الفريق على بنية تحتية تكنولوجية كافية لتمكين خدماته، بما في ذلك التدابير المناسبة لحماية تلك البنية التحتية من تدخل أطراف خارجية.

واجب جمع البيانات المسؤول

جمع البيانات ضروري للتصدي للحوادث، ولكن ينبغي تحقيق التوازن بين هدف التصدي للحوادث واحترام أصحاب المصلحة في البيانات. وأثناء التحقيق، قد يتغير مقدار المعلومات اللازم جمعها. وإذ تدور عجلة العمل خلال حادث، ينبغي لأعضاء الفريق تعديل ما يجمعونه من بيانات وفق تغير الحاجة.

وينبغي استبعاد البيانات غير ذات الصلة المباشرة بالحادث وبمعالجته من الإبلاغ.

وينبغي التعامل مع البيانات التي جُمعت واستُخرجت وفقاً للقوانين المعمول بها واحترام خصوصيات المستخدم (المستخدمين). وينبغي طلب الإذن قبل جمع البيانات ومعالجتها تحت سيطرة مالك البيانات. وينبغي احترام القوانين واللوائح المعمول بها في التعامل مع البيانات.

والبيانات التي يمكن أن تساعد أفرقة التصدي الأخرى في جهودها المتعلقة بحوادث أخرى، ينبغي أن تتاح لها، ربما في شكل منقح. وينبغي الا تتاح المعلومات المكتومة ومسجلة الملكية إلا مشفوعةً بالحمايات المناسبة.

وقبل إطلاع أطراف ثالثة على البيانات، تنبغي موازنة المخاطر مقابل الفوائد للتخفيف من المخاطر. وينبغي عدم تبادل البيانات إلا إذا رجحت كفة الفوائد بوضوح على كفة المخاطر. وينبغي تخزين البيانات الحساسة بحيث يمكن إتلافها بسهولة بعد إغلاق ملف الحادث. وينبغي إتلاف البيانات التي جُمعت بأمان وفقاً لسياسات الاحتفاظ بالبيانات.

واجب الاعتراف بحدود الولاية القضائية

ينبغي لأعضاء الفريق الاعتراف بحدود الولاية القضائية، وبالحقوق والقواعد القانونية، وبسلطات الأطراف المشاركة في الأنشطة ذات الصلة بالتصدي للحوادث واحترامها.

ويمكن أن تختلف بين الولايات القضائية المعنية القوانين واللوائح والمسائل القانونية الأخرى، كتلك المتعلقة بحماية الخصوصيات أو الإخطارات بشأن خرق البيانات. ويمكن تحديد حدود الولاية القضائية من خلال المواقع الفعلية للأطراف المعنية، مثل بلدانهم أو أماكن إقامتهم، بالإضافة إلى عوامل أخرى تتعلق بتلك الأطراف. وحتى ضمن بلد واحد، يمكن أن تختلف القوانين واللوائح بين الأقاليم السياسية (بين فرادى الولايات في الولايات المتحدة الأمريكية على سبيل المثال) أو بين الشركات أو الصناعات أو القطاعات المختلفة ضمن تلك الدولة (مثل الرعاية الصحية والخدمات المالية والمرافق الحكومية). ويمكن أن تناط بأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) الوطنية مسؤوليات و/أو سلطات محددة بشأن الأنشطة التي تشارك فيها الجهات التي تخدمها ضمن نطاق ولايتها القضائية، ويمكن أن تتعاون أيضاً مع كيانات أخرى ذات سلطة بشأن الولايات القضائية العابرة للحدود، أو أن "تسلمها" المعلومات والأنشطة.

وينبغي أن يكون أعضاء الفريق على دراية بالإشكالات الرئيسية التي تؤثر على الولايات القضائية المعنية، بما في ذلك على سبيل المثال لا الحصر، لوائح الخصوصيات أو متطلبات الإخطار بخرق البيانات. ونظراً لأن قوانين ولوائح الأمن السيبراني والخصوصيات تتطور ويتواصل تحديثها في جميع أنحاء العالم، يُستصوب التشاور مع مستشار قانوني مستنير للحصول على إرشادات كلما تضمنت القضايا حدوداً قضائية متعددة.

واجب الاستدلال القائم على الأدلة

ينبغي أن تعمل الأفرقة على أساس الوقائع التي يمكن التحقق منها. وعند تبادل معلومات، مثل مؤشرات الخرق (IOC) أو أوصاف الحوادث، ينبغي لأعضاء الفريق عرض الأدلة والنطاق بشفافية. وإذا تعذر ذلك، ينبغي أن تُشفع المعلومات ببيان أسباب عدم عرض هذه الأدلة والنطاق.

وينبغي لأعضاء الفريق تحاشي نشر الشائعات أو تناقلها. وتنبغي الإشارة إلى أي فرضية بوضوح على أنها مجرد فرضية.

وتُعتبر عمليات الأدلة والاستدلال الشفافة مهمة حتى في حالة التناقل المؤتمت، ومثال ذلك، أثناء التناقل المؤتمت لكميات كبيرة من المعلومات. وفي هذه الحالة، ينبغي إبلاغ وصف عملية التنقيب في البيانات بمستوى مفهوم من التفاصيل.

التذييل A

التعامل مع المعضلات

يمكن أن يجد أعضاء الفريق أنفسهم في كثير من الأحيان في موقف لا يبدو فيه أي إجراء ملبياً لجميع المبادئ الأخلاقية. وفي مثل هذا الموقف، ينبغي تحديد ماهية المبادئ التي ستولى الأولويات. وفي هذه الحالة، يشجع معالجو الحوادث على التفكير في أصحاب المصلحة، وكيف يمكن أن يتأثر أصحاب المصلحة هؤلاء بإجراءاتهم، ويفضل القيام بذلك في معرض نقاش مع أحد الزملاء. وكقاعدة، عامة ينبغي اختيار الحل الذي يقلل من انتهاك مدونة القواعد هذه إلى أدنى حد. وقد يتعذر ذلك في بعض الأحيان، بسبب ضغوط خارجية على سبيل المثال. وفي مثل هذه الحالة، يوصى بالمضي قدماً، مع الإشارة إلى المعضلة الأخلاقية، وربما في إطار احتجاجي.