OCHA centre for humdata

مركز البيانات الإنسانية

سلسلة المذكرات الإرشادية

مسؤولية البيانات في العمل الإنساني

الملاحظة التوجيهية حول أمان البيانات في إدارة البيانات التشغيلية

النقاط الرئيسية:

- أمن البيانات هو عنصر أساسي في المسؤولية تجاه البيانات - أي إدارة آمنة وأخلاقية وفعالة للبيانات في الاستجابة الإنسانية.
- هناك تهديدان شائعين لأمن البيانات في العمل الإنساني، مثل المراقبة والتسجيل الرقمي والنشاط غير المصرح به أو الخبيث.
- تواجه الجهات الإنسانية العديد من التحديات المتعلقة بأمنالبيانات، بما في ذلك ثغرات الأجهزة والتطبيقات والشبكات غير المؤمنة بشكل جيد، وتعرض البيانات الوصفية للخطر، والضعف الجسدي، وقدرات وأخطاء الموظفين، وإدارة البيانات الحساسة.
- ويؤدي الافتقار إلى أمن البيانات القوي إلى تقويض القدرة على تقديم المساعدة والحماية للأشخاص المتضررين، والحفاظ على واجب الرعاية للموظفين، والعمل بشكل فعال في البيئات المعقدة.
- يتطلب أمن البيانات اتخاذ إجراءات فردية ومشاركة واستثمارات تنظيمية أوسع نطاقًا. ويشمل ذلك تبني السياسات والمبادئ التوجيهية وإجراءات التخفيف ذات الصلة بالمخاطر، والاستثمار في إدارة البيانات المسؤولة، وتعزيز الإجراءات المتعلقة بمسؤولية البيانات بين الموظفين والشركاء.

مقدمة

أمن البيانات هو جزء أساسي من مسؤولية البيانات - أي إدارة آمنة وأخلاقية وفعالة للبيانات في الاستجابة الإنسانية. يتضمن ذلك مجموعة من التدابير الفعلية والتكنولوجية والإجرائية التي تحمي سرية البيانات وسلامتها وتوفرها، وتمنع فقدانها أو تدميرها أو تغييرها أو الحصول عليها أو الكشف عنها عن طريق الخطأ أو العمد أو بطرق غير قانونية أو غير مصرح بها.[1]

ان التقنيات الرقمية مثل تطبيقات الهاتف المحمول والمنصات على الويب وأنظمة التسجيل البيومترية يمكن أن تعزز العمل الإنساني، لكنها قد تزيد أيضًا من خطر اعتراض البيانات وتتبعها والوصول غير المصرح به. أظهرت الحوادث الحرجة مثل الهجوم السيبراني على خوادم اللجنة الدولية للصليب الأحمر والهلال الأحمر الدولي[2] التي تحتوي على بيانات متعلقة بخدمات استعادة روابط العائلات الخاصة بالحركة أن القطاع الإنساني يحتاج إلى التحضير للتعامل مع انتهاكات أمن البيانات الكبرى والتهديدات المرتبطة بها.

يضعف نقص أمن البيانات القوي القدرة على تقديم المساعدة والحماية للأشخاص المتأثرين، والحفاظ على الرعاية اللازمة للموظفين، والعمل بشكل مسؤول في بيئات إنسانية معقدة. يجب على المنظمات الإنسانية والموظفين فهم نقاط الضعف المتعلقة بأمن البيانات وتنفيذ إجراءات مناسبة للتخفيف من المخاطر. هذا مهم بشكل خاص في بيئات النزاعات.

تقدم هذه الملاحظة التوجيهية تهديدات شائعة لأمن البيانات والضعف في إدارة البيانات التشغيلية، وتقدم مجموعة من الإجراءات الموصى بها لتحسين أمن البيانات في البيئات الإنسانية.[3]

[1] IASC, 2021. Operational Guidance on Data Responsibility in Humanitarian Action.

[2] ICRC, 2022. ICRC cyber-attack: Sharing our analysis.

[3] إدارة البيانات التشغيلية تتضمن جمع أو استلام البيانات، وتخزينها، ومعالجتها، وتحليلها، ومشاركتها، واستخدامها، والاحتفاظ بها وتدميرها من قبل الجهات الإنسانية. IASC، ٢٠٢١. الإرشادات التشغيلية بشأن المسؤولية تجاه البيانات في العمل الإنساني.

التهديدات الشائعة لأمن البيانات

هناك تهديدان شائعان لأمن البيانات في العمل الإنساني وهما المراقبة الرقمية والتنصت والنشاط غير المصرح به أو الضار.

- إن المراقبة المستهدفة، والتي غالبًا ما يتم تمكينها من قبل مزويي خدمات الاتصالات الخاضعين لطلبات التنصت، قد تسمح لوكالات إنفاذ القانون والأمن في الدولة بالوصول إلى الاتصالات/اعتراضها. كما قد تقوم الجهات الفاعلة الحكومية وغير الحكومية على حد سواء بنشر أدوات مراقبة سرية، مثل التخفي في هيئة أبراج هواتف محمولة شرعية تُعرف باسم "IMSI-catchers"، لدعم التنصت على اتصالات الهاتف المحمول. وبعيدًا عن المراقبة المستهدفة، تجمع العديد من منصات التواصل الاجتماعي معلومات عن مستخدميها، وهذه البيانات معرضة لنفس مستوى الاستغلال مثل أي بيانات أخرى. وغالبًا ما يكون للمستخدمين رأي ضئيل أو لا شيء في قبول التحديثات على سياسات معالجة البيانات، وغالبًا ما يجهلون البيانات التي يتم إنشاؤها ومعالجتها بواسطة المنصات التي يستخدمونها أو من لديه حق الوصول إلى بياناتهم. أصبحت وفرة المعلومات التي يمكن الحصول عليها أو استنتاجها أو استنباطها من بيانات وسائل التواصل الاجتماعي شائعة بشكل متزايد لدى كل من الأطراف الخاصة والعامة للمراقبة وغيرها من الأهداف غير الإنسانية.[4]

- النشاط غير المصرح به أو الخبيث: يمكن أن تسمح هجمات التصيد الاحتيالية التي تقنع الأفراد بالنقر على رابط في الاتصالات التي تبدو وكأنها تأتي من مصادر موثوقة بالوصول عن بُعد إلى جهاز أو العبث بمحتوياته. قد يتم تثبيت البرمجيات الخبيثة على جهاز عن بعد أو من روابط مخترقة تُرسل عبر تطبيقات المراسلة والبريد الإلكتروني والمرفقات.

وتزيد الثغرات الموضحة أدناه من احتمالية حدوث هذه التهديدات.

نقاط الضعف الشائعة في إدارة البيانات التشغيلية

على الرغم من أن إدارة البيانات تختلف حسب السياق والمنظمة، إلا أن هناك عدة نقاط ضعف شائعة يواجهها العاملون في المجال الإنساني. يجب على العاملين الإنسانيين تقييم نقاط الضعف هذه وتقليلها للحد من تعرض الأشخاص المتضررين والموظفين للتهديدات والمخاطر المحتملة.

١. نقاط الضعف في الأجهزة والتطبيقات

إن استخدام أدوات أو برامج غير معتمدة أو غير خاضعة لفحص من قبل مؤسستك يحمل مجموعة من المخاطر المتعلقة بأمن البيانات. وعلى نحو مماثل، يمكن استغلال البرامج القديمة أو التي تم تكوينها بشكل سيئ لأغراض المراقبة من خلال السماح للمهاجمين بالسيطرة على الجهاز من خلال ضوابط أمنية غير كافية.

بالإضافة إلى ذلك، غالبًا ما تحتوي الأجهزة المحمولة على عدد من التطبيقات التي تمكن من المراقبة من خلال دعم تتبع النشاط والمحتوى، ونقل بيانات الموقع الجغرافي والبيانات الوصفية الأخرى إلى أطراف ثالثة. ينطبق هذا بشكل خاص على التطبيقات المجانية، التي غالبًا ما تعتمد على نموذج أعمال يستغل البيانات الشخصية. يمكن أن تحتوي إعدادات التطبيقات الافتراضية أيضًا على نقاط الضعف مدمجة مثل تعطيل تشفير الرسائل بشكل افتراضي، أو تشغيل النسخ الاحتياطي للسحابة، أو استخدام وظيفة تسجيل المؤتمرات، مما يؤدي إلى تخزين المحادثات على خوادم الطرف الثالث.

٢. الشبكات غير المؤمّنة بشكل جيد

استخدام الشبكات العامة أو الشبكات المفتوحة Wi-Fi (أي تلك التي غير محمية بكلمة مرور) قد يعرض العاملين في المجال الإنساني للمراقبة وقد يؤدي أيضًا إلى التطفل، مثل انضمام أطراف غير مصرّح لها إلى محادثات جماعية أو اجتماعات عبر الإنترنت. يمكن أن تنشأ نقطة لبضعف هذه أيضًا عندما لا تكون المنظمة قد قامت بتكوين خوادمها وموجّهاتها وخدماتها بشكل جيد. غالبًا ما تكون الإعدادات الافتراضية متساهلة جدا وقد تسمح للمهاجمين بالوصول إلى الأجهزة والشبكات. يمكن أن يكون هدف هذا النوع من التطفل هو تحديد وتصنيف الأجهزة والمستخدمين على الشبكة وموقعهم الجغرافي والأشخاص الذين تواصلوا معهم، وحتى محتوى التواصل.

[4] Privacy International, 2020. Privacy shouldn't be a luxury; also Privacy International, 2019. Buying a smartphone on the cheap? Privacy might be the price you have to pay.

٣. تعريض البيانات الوصفية

تترك جميع الأنشطة الرقمية آثارًا رقمية، غالبًا ما يشار إليها باسم البيانات الوصفية، على الأجهزة والخوادم والبنية الأساسية للشبكة. تصف البيانات الوصفية المعلومات المتعلقة بالبيانات المعنية. على سبيل المثال، عند إرسال بريد إلكتروني، تشمل البيانات الوصفية الوقت المرسل فيه وعناوين IP للمرسل والمستلم. تولد المنظمات الإنسانية البيانات الوصفية بشكل سلبي من خلال الاتصالات الداخلية، والتبادل مع الأشخاص المتضررين من الأزمات، وأثناء تنفيذ البرنامج ومراقبته.[٥] يمكن أن يكون الوصول إلى مثل هذه البيانات الوصفية متطفلاً وفاضحًا مثل الوصول إلى أي بيانات أخرى. يمكن أن تكشف عن معلومات حول الأفراد مثل موقعهم وأنشطتهم الأخيرة مما يمكنهم من إعادة التعرف عليهم واستهدافهم من قبل الجهات الضارة.

٤. نقاط الضعف المادية

هناك عدد من الثغرات المادية التي قد تؤدي إلى وصول غير مصرح به إلى البيانات والمعلومات من قبل جهات ضارة.على سبيل المثال، قد يواجه الموظفون نقاط فحص تطلب منهم تسليم الأجهزة والوثائق. هناك أيضًا خطر من المراقبة المادية: يمكن لأي شخص بالقرب من الاجتماع مع محاور أن يسمع المناقشات أو يستمع بشكل متعمد إلى المحادثة. أخيرًا، تكون الأجهزة معرضة لخطرللضياع أو السرقة عند اخراجها من بيئات المكاتب المؤمنة.

٥. درات الموظفين والأخطاء

إن الممارسات السيئة والتطبيق غير المتسق لتدابير أمن البيانات من الممكن أن يؤدي إلى تفاقم نقاط الضعف القائمة أو خلق نقاط ضعف جديدة.. قد لا يكون الموظفون على دراية لنقاط الضعف المتعلقة بأمن البيانات وكيفية التخفيف من المخاطر المرتبطة بها. كما قد يكون لقيود الموارد والوقت تأثيرات سلبية أيضًا على كيفية التعامل مع البيانات من قبل الموظفين عند التركيز على مجالات العمل الأخرى. على سبيل المثال، قد يشارك الموظفون بيانات حساسة دون تشفير الملف (أي يتطلب كلمة مرور لفتحه) مما يزيد من خطر تعريض البيانات عن غير قصد.

٦. إدارة البيانات الحساسة

تُشكل البيانات الحساسة، مثل البيانات المستمدة من مسوحات الاسر وتقييمات الاحتياجات وغيرها من أشكال البيانات الصغيرة، حجمًا متزايدً الاهمية من البيانات افي القطاع الإنساني. بينما هذا النوع من البيانات يشكل اهمية بالغة للعمل الإنساني، فإنه قد يتسبب في أضرار جسيمة للأفراد أو المنظمات إذا تم الوصول إليه دون الحصول على إذن مناسب. تؤدي إدارة البيانات الحساسة الى تفاقم نقاط الضعف الأخرى من خلال زيادة شدة الضرر المحتمل. كما يمكن أن تزيد من احتمالية وقوع هجمات مستهدفة، بما في ذلك التدخل والوصول غير المصرّح به.[٦]

[5] Privacy International and ICRC, 2018. The Humanitarian Metadata Problem - Doing No Harm in the Digital Era.

[٦] يمكن أن تكون البيانات الشخصية وغير الشخصية حساسة على حد سواء. لمزيد من المعلومات، انظر IASC، ٢٠٢١. الإرشادات التشغيلية بشأن المسؤولية تجاه البيانات في العمل الإنساني.

الإجراءات الموصى بها لأمن البيانات

يجب على العاملين في القطاع الإنساني اتخاذ الإجراءات التالية لتحسين أمن البيانات في عملهم.

فهم المخاطر في بيئتك الخاصة

- تحديد المخاطر وتقييمها من خلال إجراء تقييم تأثير البيانات (DIA).[٧] توفر تقييمات تأثير البيانات فهمًا للعواقب المحتملة لنشاط إدارة البيانات.
- اعادة تصميم أو إلغاء نشاط إذا كانت المخاطر المتوقعة لإدارة البيانات تفوق الفوائد المقصودة.
- استشارة الأخبار والاحاطات وتقارير الامن ذات الصلة بانتظام لإعلام فهم للمخاطر في بيئتك.
- تكييف نهجك و خياراتك مع الوضع. قد تكون الأداة أو التكنولوجيا مناسبة في سياق ما، ولكنها غير مناسبة في سياق آخر.

ممارسة إدارة جيدة لكلمات المرور

- تامين أجهزتك وحساباتك باستخدام كلمات مرور قوية تتضمن أرقامًا واحرفا كبيرة وصغيرة ورموزًا تتكون من ١٦ حرفًا على الأقل لكل كلمة مرور
- تمكين المصادقة الثنائية المصادقة الثنائية لجميع الحسابات.
- عدم إعادة استخدام نفس كلمة المرور لحسابات متعددة وتحديث كلمات المرور بانتظام (ما لم يتم استخدام المصادقة الثنائية).
- عدم تخزين كلمات المرور الخاصة بك بشكل مادي (على ملاحظات) أو رقميًا (في ملف على جهازك) وعدم مشاركة كلمة المرور مع الآخرين.
- لا تقم بتفعيل خاصية 'تذكرني' في التطبيقات والمتصفحات.
- استخدام مدير كلمات المرور، ويفضل أن يكون واحدًا موصى به أو معتمدًا أو مُدارًا من قبل منظمتك.
- استخدام خدمة مراقبة تسرب كلمة المرور للتحقق بشكل منتظم مما إذا كلمة مرورك قد تعرضت للاختراق.
- تغيير كلمات المرور على جميع الحسابات على الفور إذا فقدت جهازك أو سُرق.
- استخدام علامات تبويب المتصفح الخفية أو الخاصة بقدر الإمكان.

استخدام برامج مكافحة الفيروسات / مكافحة البرامج الضارة

- تأكد من وجود برنامج مكافحة الفيروسات / مكافحة البرامج الضارة المناسب على جميع الأجهزة.
- تحقق دائمًا مع أخصائي تكنولوجيا المعلومات في مكتبك إذا كان متوفرًا أو استشر زملاءك في منظمة شريكة لتحديد الأداة المناسبة وضبطها بشكل مناسب.

الحفاظ على تحديث البرامج وأنظمة التشغيل

- تحقق بانتظام من أن جهازك وبرامجك وتطبيقاتك وإضافات المتصفح لديك محدثة، وتمكين التحديثات التلقائية لنظام التشغيل لديك.
- استخدم متصفحات الويب التي تتلقى تحديثات أمان تلقائية.
- تجنب استخدام البرامج التي من المحتمل ألا تتوفر صيانتها في المستقبل.
- أغلق الأجهزة بانتظام أو عندما يُطلب منك ذلك من قبل نظامك لتمكين التحديث وحماية نفسك من الهجمات.

تجنب عمليات احتيال التصيد وكن حذرًا فيما تنقر عليه

- عند تلقي رسائل بريد إلكتروني مشبوهة أو رسائل أخرى، تحقق دائمًا من عنوان المُرسِل / معلومات الاتصال به وانقر فقط على الروابط أو المرفقات من المُرسلين الموثوق بهم.

[٧] انظر إلى مذكرة التوجيه حول تقييم تأثير البيانات للمزيد من المعلومات حول كيفية إجراء تقييم تأثير البيانات (DIA).

- حتى إذا كان الرابط من مُرسِل موثوق به، انسخه دائما واستخدم علامة تبويب متصفح خاصة أو متخفية لفتحه.
- تحقق دائمًا من أن عنوان URL يتوافق مع موقع ويب معروف وذو سمعة طيبة من خلال تشغيله من خلال تشغيله من خلال محرك بحث للتأكد من أن الموقع الإلكتروني شرعي.
- مرر الماوس فوق رابط URL قبل النقر فوقه لمعرفة المكان الذي يأخذك إليه الرابط بالفعل.
- لا ترد على رسائل البريد الإلكتروني المشبوهة أو إعادتها لزملائك.
- ابلغ عن أي نشاط مشبوه من خلال القناة المناسبة داخل منظمتك.

استخدام الأجهزة المحمولة بشكل مسؤول

- استخدام أجهزة منفصلة لأغراض العمل كلما أمكن ذلك. احتفظ بأجهزة العمل في مكان آمن في جميع الأوقات وتجنب حملها دون داعي.
- استخدم أدوات المراسلة المعتمدة من قبل منظمتك والتي توفر تشفير من البداية إلى النهاية.
- قلل من استخدام اتصال البلوتوث وخدمات الموقع، وأوقف تشغيلها عند الإمكان.
- استخدام شبكة افتراضية خاصة (VPN) عند العمل عبر الإنترنت. استشر قسم تكنولوجيا المعلومات أو زملائك للحصول على قائمة بالأدوات المعتمدة.
- قم دائمًا بتسجيل الخروج من حسابك (حساباتك) إذا كنت تستخدم جهاز كمبيوتر ام جهازا عاما/ مشتركا.
- لا تقم بالوصول إلى الخدمات أو المعلومات الحساسة على الأجهزة العامة/المشتركة إلا إذا كان ذلك ضروريًا للغاية.
- قم بتعطيل ميزات إلغاء القفل البيومترية - خاصة أثناء التنقل.
- تاكد أن جهازك لا يتتبع النشاط أو المحتوى قم بتعطيل هذه حيثما امكن.

ممارسة تقليل البيانات الى الحد الادنى

- جمع الحد الأدنى فقط من البيانات المطلوبة لتحقيق الهدف والأغراض لنشاط إدارة البيانات المعين.
- الاحتفاظ فقط بالبيانات الحساسة فقط عند الضرورة القصوى ولفترة زمنية ضروية لتحقيق الغرض الذي يتم ادارتها من أجله وكما هو مطلوب بموجب الإرشادات والقانون والتنظيمات المعمول بها.

حماية البيانات الحساسة

- قم بنقل وتخزين البيانات باستخدام أدوات وقنوات معتمدة (محليًا على خادم داخلي أو جهاز كمبيوتر أو كمبيوتر محمول، أو على خوادم وأنظمة تديرها منظمتك، باستخدام التشفير من البداية الى النهاية).
- حماية الملفات (Word، Excel، PDF) التي تحتوي على بيانات حساسة بكلمة مرور و/او تشفيرها ومشاركة كلمات مرور المستندات من خلال قنوات منفصلة (على سبيل المثال، إرسال كلمة مرور نصية لمستند مرسل عبر البريد الإلكتروني).
- تحديد عدد الأشخاص الذين يمكنهم الوصول إلى البيانات الحساسة ومراقبتهم بعناية.
- حدد جدولًا زمنيًا لاحتفاظ وتدمير كل البيانات التي تديرها منظمتك واستخدم الأدوات المناسبة لتدمير البيانات.
- لا تناقش المعلومات الحساسة في الأماكن العامة وتأكد من عدم وجود أشخاص غير مصرح لهم الوصول إلى مساحات الاجتماع الخاصة بك، سواء كانت في الواقع أو عبر الإنترنت.
- قم بتشفير رسائل البريد الإلكتروني الخاصة بك.

- احتفظ بسجل أصول البيانات[٨] الذي يشير إلى مستوى الحساسية لكل نوع من انواع البيانات التي يديرها مكتبك. قم بمراجعة مستويات الحساسية بانتظام مع تطور السياق.
- انظر في تطوير تصنيف حساسية البيانات والمعلومات لسياقك، اما كجزء من بروتوكول[٩] مشاركة المعلومات أو كوثيقة مستقلة للرجوع إليها.[١٠]

الاستثمار التنظيمي في أمان البيانات

بالإضافة إلى الإجراءات الفردية الموضحة أعلاه، يتطلب أمن البيانات مشاركة واسعة النطاق على مستوى المنظمة. تحتاج المنظمات إلى الاستثمار في تدابير أمن البيانات لتعزيز مسؤولية البيانات في جميع مكاتبها وفرقها. وقد يشمل ذلك تبني السياسات والمبادئ التوجيهية ذات الصلة، وإجراءات التخفيف المتعلقة بالمخاطر، واستثمار الموارد البشرية والمالية في أمن البيانات وإدارتها، وتعزيز المسؤولية تجاه البيانات بين الموظفين والشركاء.

المتعاونون: الخصوصية الدولية؛ جامعة ييل، معهد جاكسون للشؤون العالمية.

ينشر مركز البيانات الإنسانية («المركز») بالتعاون مع الشركاء الرئيسيين، سلسلة من المذكرات التوجيهية وأوراق النصائح حول مسؤولية البيانات في العمل الإنساني على مدار عامي ٢٠٢٢ و٢٠٢٣. وتواصل سلسلة المذكرات التوجيهية العمل الذي بدأ في عامي ٢٠١٩ و٢٠٢٠. كما أنها تكمل الإرشادات التشغيلية للجنة الدائمة المشتركة بين الوكالات بشأن مسؤولية البيانات في العمل الإنساني وإرشادات مكتب تنسيق الشؤون الإنسانية بشأن مسؤولية البيانات، والتي نُشرت في فبراير ٢٠٢١ وأكتوبر ٢٠٢١ على التوالي. ويهدف المركز من خلال هذه السلسلة إلى تقديم إرشادات إضافية حول قضايا وعمليات وأدوات محددة لمسؤولية البيانات في الممارسة العملية. وقد أصبح من الممكن إصدار المذكرات التوجيهية وأوراق النصائح التي نُشرت في عامي ٢٠٢٢ و٢٠٢٣ بدعم من حكومة سويسرا.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

[٨] نموذج سجل الأصول البيانية للجنة الدائمة المشتركة متاح هنا.
[٩] نموذ بروتوكول مشاركة المعلومات للجنة الدائمة المشتركة متاح هنا.
[١٠] انظر على سبيل المثال إلى تصنيف الحساسية للبيانات والمعلومات لأوكرانيا.