11

إدارة المخاطر

إدارة المخاطر

تواصل الشركة التكيف مع التطور المتقدم والسريع للتكنولوجيا.، في الوقت نفسه تعمل على ضمان اعتماد إطار عمل قوي وملائم ونشط لإدارة المخاطر للتخفيف من المخاطر الفعلية والمحتملة.

تقدم إدارة المخاطر في المجموعة تقاريرها مباشرة إلى لجنة المخاطر التابعة لمجلس الإدارة (BRC)، وتوضح هذه الآلية الأهمية التي توليها المجموعة للمحافظة على استدامة الأعمال على المدى الطويل، وتشرف لجنة المخاطر التابعة لمجلس الإدارة BRC على تطبيق سياسات وإجراءات إدارة المخاطر، فهي تستعرض مدى شمولية إدارة المخاطر فيما يتعلق بالمخاطر التي تواجهها المجموعة.

تتم مراجعة التغييرات على الاجراءات و السياسات والموافقة عليها من قبل لجنة المخاطر التابعة لمجلس الإدارة BRC بصفة سنوية، ويتم مراجعة اتجاهات المخاطر على أساس ربع سنوي، وتساعد الادارات الرقابية وهي إدارة التدقيق الداخلي، حوكمة الشركات، وادارة المخاطر، بالإضافة الى لجنة المخاطر.

تقوم زين بتقييم آثارها الاجتماعية والاقتصادية والبيئية من منظور المخاطر، وقد استمرت في مواءمتها مع استراتيجية الاستدامة المؤسسية منذ العام 2019، وتأخذ هذه التقييمات في الاعتبار المخاطر والفرص المتصلة بتغير المناخ فضلا عن المخاطر الاجتماعية والاقتصادية، يتم تحديد المخاطر التي لها أكبر تأثير مادي على زين من خلال البحوث المستمرة والمشاركة الشاملة مع أصحاب المصلحة، بحيث يمكن التخطيط للتخفيف منها في مرحلة مبكرة.

يتم شرح المخاطر والفرص المتعلقة بالمناخ بتعمق أكثر في تقرير فريق العمل المعني بالإفصاحات المالية المتعلقة بالمناخ في الصفحة 119.

عضوية الجمعيات المتعلقة بالمخاطر

تشكل ادارة الشؤون التنظيمية لمجموعة زين نقطة الاتصال الوحيدة لعضوية زين في اتحاد (GSMA) والاتحاد الدولي للاتصالات (ITU)، ومن خلال هذه العلاقة، تستخدم إدارة المخاطر الموارد لعملياتها التجارية لاكتساب رؤى حول أفضل الممارسات والمعايير الدولية، وتضمن هذه الموارد أن تقوم زين بتضمين المعايير والسياسات الرائدة في عملياتها المتعلقة بالأمن في هذه الصناعة.

اتحاد (GSMA).، هو منظمة عالمية توحد منظومة الاتصالات لاكتشاف وتطوير وتقديم الابتكار التأسيسي لبيئات الأعمال الإيجابية والتغيير المجتمعي، ومجموعة زين هي عضو في الاتحاد، وتشارك في في المؤتمر العالمي للهواتف النقالة بانتظام، كما تتلقى زين معلومات وتشاركها مع نظرائها الآخرين في مجالات التجوال والربط البيني والأمن، ولدى زين أيضا عضوية في الاتحاد الدولي للاتصالات، وهي وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات، ويسهل الاتحاد الاتصالية الدولية في شبكات الاتصالات لتخصيص طيف راديوي عالمي ووضع المعايير التقنية التي تضمن التوصيل البيني للشبكات والتكنولوجيات بسلاسة، وتحسين نفاذ المجتمعات المحرومة في جميع أنحاء العالم إلى تكنولوجيا المعلومات والاتصالات.

إطار إدارة المخاطر

الشكل 1: إطار عمل زين لإدارة المخاطر (التوافق مع ISO 31000)

تواصل زين استخدام مصفوفة احتمالية التأثير لتحديد تصنيف مخاطر الأحداث التي تواجه الشركة عبر عملياتها، يتم تقييم التأثيرات عبر معايير متعددة تشمل المالية والسمعة وتغير المناخ والأسواق، والعملاء، والموظفين، وغيرها.، يأخذ التصنيف أيضا في الاعتبار الحالة «قبل» و «بعد» تخفيف المخاطر، مما يوفر معلومات عن حالة المخاطر المتأصلة والباقية.

الشكل 2: إطار عمل زين لإدارة المخاطر (التوافق مع COSO)

المبدأ التحوطي (الاحترازي)

تلتزم زين، كمبدأ احترازي، بالمتطلبات البيئية المعمول بها في تصميم منتجاتها وتقديمها للخدمات، ويعد التقدم السريع في التكنولوجيا أحد المخاطر الرئيسة للشركة، حيث تتم مراقبته من قبل لجنة المخاطر المنبثقة عن مجلس الإدارة BRC ولجنة العمل المناخي ومجلس الإدارة.، و تعتمد أعمال زين على التكنولوجيا لتطوير وتقديم منتجات وخدمات منخفضة الكربون يحتاجها العملاء، وتعمل فرق تصميم المنتجات وفرق المشتريات في الشركة مع الموردين لتطوير منتجات ذات آثار بيئية أقل، تتضمن قائمة المراجعة المستخدمة كجزء من عملية التصميم الاعتبارات المتعلقة بالمناخ مثل استخدام الطاقة والتفكيك في نهاية العمر للإصلاح أو إعادة الاستخدام.

خصوصية البيانات

تقدر الشركة معلومات التعريف الشخصية (PII) المقدمة إليها من قبل عملائها وموظفيها وموردیها وأصحاب المصلحة الآخرين، وتلتزم زين بجمع معلومات تحديد الهوية الشخصية واستخدامها والاحتفاظ بها وعدم الكشف عنها بطريقة شفافة وآمنة، من أجل الامتثال للمتطلبات القانونية والتنظيمية المعمول بها لمعالجة هذه المعلومات.

في عام 2022،، تلقت زين جنوب السودان إشعارا للأمن السيبراني من قبل الهيئة الوطنية للاتصالات، حيث تمت مشاركته مع جميع مشغلي الاتصالات في البلاد، تطلب هذا الإشعار من مشغلي الاتصالات بإجراء تقييمات المخاطر الأمنية الخاصة بهم، وقامت زين جنوب السودان بالعمل مع إدارة المخاطر في مجموعة زين، بإجراء مراجعة أمنية وتقديم توصيات بمجموعة حلول لتعزيز الأمن السيبراني.

تقوم عمليات زين بمعالجة معلومات التعريف الشخصية للعملاء لتوفير منتجات وخدمات مخصصة بناء على التركيبة السكانية وسلوك العملاء، وتصرح الشركة بأنه من الممكن تحليل بيانات استخدام العملاء لتصميم المنتجات بناء على ملفات تعريف العملاء، وتضمن الشركة أنه عند القيام بذلك، سيتم الإشارة إليه صراحة في عقد مبيعات الشركة (الشروط والأحكام) مع الامتثال أيضا لقواعد ولوائح الدولة المحددة.

يتم تزويد العملاء أيضا بإشعار خصوصية من خلال قنوات مختلفة، بما في ذلك موقع الويب وعقد البيع، بشأن معالجة بياناتهم الشخصية، يمكن العثور على معلومات إضافية حول حوكمة وسياسات خصوصية البيانات في قسم «عملاؤنا.. ومنتجاتنا » في الصفحة 77.

السياسات والممارسات المتعلقة بجمع واستخدام والاحتفاظ بمعلومات العملاء ومعلومات التعريف الشخصية

زين البحرين

حافظت زين البحرين على شهادة إدارة أمن المعلومات ISO 27001، وتؤكد هذه الشهادة صحة تطبيق زين للضوابط الأمنية لحماية معلومات العملاء، وتتضمن أمثلة عناصر التحكم في الأمان مكافحة البرامج الضارة واكتشاف نقطة النهاية وعناصر التحكم في الوصول، يمكن العثور على معلومات إضافية حول هذا الموضوع في سياسة خصوصية البيانات الخاصة بزين البحرين:
https://www.bh.zain.com/en/copyright/privacy

زين العراق

في العام 2022، أجرت زين العراق تقييمات للأمن السيبراني ونقاط الضعف، واختبار الاختراق، وتقييم أمن إشارات الاتصالات - SS7 ، وبروتوكولات GTP لحماية معلومات العملاء..

زين الأردن

هناك قانون جديد لحماية البيانات قيد المراجعة في الأردن،، بالتالي تم إجراء مناقشات مع جميع الأطراف المعنية لتقييم المخاطر حول بيانات معلومات تحديد الهوية الشخصية، مع وضع السياسات والإجراءات التصحيحية وفقا لذلك.

زين الكويت

تنطبق لائحة حماية خصوصية البيانات الخاصة بالهيئة العامة للاتصالات وتقنية المعلومات على كل من القطاعين العام والخاص الذي يقوم بجمع ومعالجة وتخزين معلومات التعريف الشخصية، في العام 2022، عينت زين الكويت مسؤولا عن خصوصية البيانات، ليكون مسؤولا عن الإشراف على الضوابط الفنية والتنظيمية المناسبة للامتثال للوائح.

زين السعودية

تخطط "زين السعودية" لتطوير ومشاركة سياسة الخصوصية مع مالكي البيانات في العام 2023، مع تحديد تفاصيل معالجة بياناتهم الشخصية، بما في ذلك الغرض من جمع البيانات وكيفية معالجة البيانات،، يتم حاليا وضع اللمسات الأخيرة على متطلبات حماية البيانات الشخصية وتقييم تأثير الخصوصية.

زين السودان

لدى زين السودان سياسات متعددة لضمان ممارسات آمنة فيما يتعلق بجمع واستخدام والاحتفاظ بمعلومات العملاء ومعلومات التعريف الشخصية، التي تشمل:

1. التدقيق الداخلي
2. مدونة قواعد السلوك
3. سياسة الإجراءات التأديبية
4. سياسة الامتثال القانوني

زين جنوب السودان

تعمل زين جنوب السودان حاليا على تطوير سياسات أمن المعلومات لحماية بيانات العملاء، من المقرر الانتهاء من السياسات بحلول النصف الأول من العام 2023.

معلومات العميل للأغراض الثانوية

وفقا لتعريف مجلس معايير محاسبة الاستدامة (SASB) للغرض الثانوي، تقوم زين بمعالجة بيانات العمليات لتصميم المنتجات لتعزيز جودة الخدمات المقدمة للعملاء، بالرغم من ذلك،، فإنه لا يتم نقل معلومات العميل واستخدام البيانات أو مشاركتها مع طرف ثالث ما لم تطلب سلطات إنفاذ القانون ذلك، في هذه الحالة يتم ذلك بأمر قضائي.

يمكن العثور على مزيد من المعلومات حول حوكمة وسياسات خصوصية البيانات في زين في قسم « خدماتنا و منتجاتنا» في الصفحة 81.

تواصل زين مراقبة الشكاوى الواردة من أطراف ثالثة وهيئات رقابية، وتحديد التسريبات وفقدان بيانات العملاء كما هو موضح في الجدول أدناه:

	الشكاوي الواردة من الأطراف الخارجية والمثبتة من قبل المنظمة	شكاوى من الهيئات التنظيمية	العدد الإجمالي للتسريبات أو السرقات أو الخسائر المحددة لبيانات العملاء
زين البحرين	0	0	0
زين العراق	0	0	0
الأردن	2	0	*2
زين الكويت	0	0	0
زين السعودية	0	0	0
زين السودان	0	0	0
زين جنوب السودان	0	**1	0

* الحادثتان في الأردن كانتا بسبب السلوك البشري ونقص الوعي بتدابير الرقابة على الرغم من الضوابط المطبقة، فيما يلي موجز لهذه الحوادث:
- تسرب معلومات العميل من قبل ممثلي المتجر.
- تسرب معلومات العميل من قبل التجار.
- تأثر عميل واحد فقط بسبب تسرب البيانات

** توفر الهيئة الوطنية للاتصالات هذه المعلومات لتمكين الجهات المتضررة من إجراء تقييم المخاطر الأمنية الخاصة بها وتحليل الحوادث، ومن ثم اتخاذ الإجراءات المناسبة لتطهير الأنظمة، والشبكات المصابة وتأمين أنظمتها وشبكاتها.

أمن البيانات

واصلت زين بذل جهود كبيرة لحماية موظفيها وعملائها من هجمات التصيد المتعددة من خلال تمكين الميزات التي يمكن للمستخدمين من خلالها الإبلاغ عن مثل هذه الهجمات ورسائل البريد الإلكتروني غير المرغوب فيها من خلال نقرة زر واحدة، مما يجعل عملية التحقيق أكثر كفاءة ويسمح باتخاذ إجراءات فورية..

نهج الإدارة لتحديد ومعالجة مخاطر أمن البيانات

تعتبر البنية التحتية لشركة زين بالغة الأهمية لأنها تعالج وتخزن معلومات سرية وقيمة للغاية معرضة للاستهداف بشكل كبير من قبل مجرمي الإنترنت، ومع تطور التكنولوجيا على مستوى العالم، تتطور التهديدات السيبرانية، مما يؤدي إلى مجموعة متنوعة من الآثار السلبية على الأفراد والمؤسسات والمجتمعات.

للتخفيف من احتمالية وتأثير الهجمات السيبرانية والحد منها، طورت زين المرونة الإلكترونية، وهي القدرة على تحديد تهديدات الأمن السيبراني الكارثية المحتملة والحماية منها واكتشافها والاستجابة لها، والتعافي منها بشكل فعال، لتحقيق المرونة السيبرانية، يجب على زين تحديد المخاطر بشكل فعال وتصميم ضوابط قوية وقياس الفعالية باستمرار لتكون قادرة على خلق بيئة تشغيل مستدامة وآمنة.

فيما يلي توضيح لإطار العمل المشار إليه في استراتيجية زين للمرونة الإلكترونية:

تتضمن بعض الأمثلة على مبادرات الأمن السيبراني عبر أسواق زين:

- تقييمات الأمن السيبراني/ اختبار الاختراقات و تقييمها
- اختبار الاختراق
- تقييم أمن إشارات الاتصالات
- الإبلاغ عن جميع الحوادث والمخالفات الأمنية إلى الجهاز القومي لتنظيم الاتصالات
- شهادة نظام إدارة أمن معلومات ISO 27001
- تدريب أمن المعلومات لجميع الموظفين

إدارة المخاطر النظامية الناجمة عن الاضطرابات التكنولوجية

تتطلب خدمة المهام الحرجة تواجداً مستمراً في الأوقات التي لا يُسمح فيها بتوقف الخدمة، الذي قد يؤدي إلى ضرر فوري وكبير، وتواصل زين مراقبة أي اضطرابات تحدث في جميع أنظمتها الرئيسية:

مجموعة زين	
نظام	توافر
تخطيط موارد المؤسسات	%100
أوراكل هايبريون	%100
موقع zain.com	%99.99

زين البحرين	
نظام	توافر
خدمة الفوترة / CRM	%100
الشحن	%100
توزيع القسائم الالكترونية	%100
موقع bh.zain.com	%100

زين العراق	
نظام	توافر
الفواتير	%100
الشحن	%100
توزيع القسائم الالكترونية	%100
موقع iq.zain.com	%100

زين السعودية	
نظام	توافر
الفواتير	%99.9996
الشحن	%99.9996
توزيع القسائم الالكترونية	%99.9996
موقع sa.zain.com	%99.9996

انتظر الأردن	
نظام	توافر
الفواتير	%100
الشحن	%100
توزيع القسائم الالكترونية	%100
موقع jo.zain.com	%100

زين السودان	
نظام	توافر
الفواتير	%100
الشحن	%100
توزيع القسائم الالكترونية	%100
موقع sd.zain.com	%100

زين الكويت	زين السودان
نظام	توافر
الفواتير	%99.95
الشحن	%99.95
توزيع القسائم الالكترونية	%99.95
موقع kw.zain.com	%99.95

زين جنوب السودان	
نظام	توافر
الفواتير	%100
الشحن	%100
توزيع القسائم الالكترونية	%100
موقع ss.zain.com	%100

وصف الأنظمة لتقديم الخدمة دون عوائق أثناء انقطاع الخدمة

1. توزيع القسائم الإلكترونية – وهو نظام للتحقق من الرصيد وتحويله من جانب العملاء من المتاجر والموقع الإلكتروني وغير ذلك، لإعادة شحن حساباتهم للمكالمات والبيانات وما إلى ذلك، هذا النظام يستخدمه عملاء الدفع المسبق فقط.
*قناة رقمية لاكتشاف الخدمات وشراء الأجهزة والاشتراكات وإعادة الشحن، تُستخدم من جانب عملاء الدفع المسبق والدفع الآجل.

2. Zain ERP – أداة تخطيط موارد المؤسسات الشاشة - وقت التشغيل بالثواني / الشهر (30 * 24 * 60 * 60 ثانية)

3. أوراكل هايبريون - أداة التخطيط المالي والميزانية الأساسية الشاشة - وقت التشغيل بالثواني / الشهر (30 * 24 * 60 * 60 ثانية)

4. قناة موقع زين - قناة رقمية لاكتشاف الخدمات وشراء الأجهزة والاشتراكات وإعادة الشحن، تُستخدم من جانب عملاء الدفع المسبق والدفع الآجل. - وقت تشغيل موقع الويب بالثواني / الشهر (30 * 24 * 60 * 60 ثانية)

5. الفوترة / CRM: نظام الفوترة الداخلي المستخدم لمعالجة والتحقق من صحة سجلات الفواتير والفواتير والتكامل والتسوية مع أنظمة المحاسبة الأخرى.

6. شبكة الشحن: تسمح الشبكة الذكية بتوزيع الوظائف بمرونة في مجموعة متنوعة من العمليات داخل وخارج الشبكة، كما تسمح بتعديل البنية للتحكم في الخدمات، يمكن لهذه الشبكات فصل الخدمات الإضافية عن نظام تبديل المكالمات، مما يسهل إضافة خدمات مستخدم جديد مثل فحص أو انتظار المكالمات، بالإضافة إلى خدمات أكثر تعقيدا مثل الشحن المتغير، وخدمات معرف المتصل والرسائل الدولية.

التدريب على المخاطر الأمنية

مع استمرار التطورات فائقة السرعة في المجالات التكنولوجية.، أصبح من الصعب إدراك الأشكال الجديدة للهجمات الإلكترونية، وكجزء من برنامج «**نتوقف. فكر. اتخذ إجراء**» للتوعية بالأمن السيبراني في زين ، تواصل الشركة رفع مستوى الوعي فيما يتعلق بتزايد وتيرة مثل هذه الهجمات.

تحتفظ زين باشتراكات في الإشعارات والتنبيهات التي يتم إنشاؤها من منصة مشاركة معلومات البرامج الضارة التابعة لمركز تحليل معلومات الاتصالات التابع لاتحاد GSMA، وبما أن الهجمات السيبرانية تتطور باستمرار وتنمو على مستوى التعقيد والحجم، فإن معلومات التهديد المتوفرة لدى زين عبر هذه المنصة تساعد المؤسسة على أن تكون استباقية في دفاعاتها السيبرانية، واتخاذ الخطوات اللازمة لحماية زين وشركاتها العاملة من الاختراق.

تحديثات التوعية للعام 2022

	المجموعة	الكويت	السعودية	البحرين	العراق	الأردن	السودان	جنوب السودان
مجموع الموظفين	200	1,478	1,752	195	1,069	1,211	783	116
إجمالي عدد الموظفين الذين تلقوا محتوى توعويا	200	1,478	1,752	195	1,069	1,211	783	116
إجمالي عدد القنوات المستخدمة	3	1	3	4	1	4	3	3
القنوات المستخدمة	البريد الإلكتروني للشركات النشرة الإخبارية الرسائل القصيرة	البريد الإلكتروني للشركات النشرة الإخبارية	البريد الإلكتروني للشركات النشرة الإخبارية الشاشات الإرشادية تمرين الاحتيال الالكتروني	البريد الإلكتروني للشركات، النشرة الإخبارية، لافتات رقمية، ورش عمل مادية، جلسات عبر الإنترنت	جلسة تعريفية	البريد الإلكتروني للشركات، النشرة الإخبارية، مقاطع ألعاب الفيديو، جلسات رفع الوعي	البريد الإلكتروني للشركات، النشرة الإخبارية، التحفيز الإسبوع المعلوماتي	البريد الالكتروني للشركات، النشرة الإخبارية، الملصقات، الرسائل القصيرة

* تلقى جميع الموظفين على مستوى المجموعة محتوى توعية أمنية حول التخفيف من المخاطر الأمنية

موضوعات أمن المعلومـــات التي تمت تغطيتها والتخطيط لها في العام 2022 :

- هجمات رموز QR
- هجمات البلوتوث
- التهديدات الداخلية
- كلمات المرور والمصادقة الثنائية
- تحديثات التطبيق
- الأمن المادي
- تحميل الملفات الضارة
- هجوم انتحال الشخصية
- التطفل على البيانات
- عمليات الاحتيال عبر الإنترنت

تتألف القائمة التالية من الدورات التدريبية للأمن السيبراني التي يأخذها موظفو إدارة المخاطر في جميع العمليات:

- مدير أمن المعلومات المعتمد - CISM
- مهندس حلول خدمات الويب من أمازون - مشارك
- تخصص أمن خدمات الويب من أمازون
- ISO 27001 المنفذ الرئيسي
- دورة إعداد مدير أمن المعلومات المعتمد
- قيادة وإدارة الأمن السيبراني
- إدارة المخاطر المؤسسية
- ISO 22301 BCM
- التدريب على جدار حماية تطبيقات الويب (باراكودا)
- النقاط الجوهرية في الهندسة الاجتماعية 2022
- ورشة عمل أمن الاتصالات
- مجال الهجوم الخارجي أكبر مما تعتقد
- فورتينت سريع وآمن 2022
- الهكر الأخلاقي المعتمد (CEH)
- مهندس أمن تطبيقات معتمد (CASE.net)
- Zain Talk - التوعية بحماية خصوصية البيانات
- تنفيذ إطار عمل إدارة المخاطر NIST

المبادرات مع أصحاب المصلحة الخارجيين

المبادرة	تاريخ التبني	الشركات المشغلة المعنية	طبيعة المبادرة (إلزامية / طوعية)	أصحاب المصلحة المعنيين
ختم اعتماد الصيانة والتشغيل	20-مايو-2019	زين الكويت	طوعية	الخدمات المهنية لمعهد الجهوزية
نظام إدارة أمن المعلومات أيزو 27001:2013	10-يناير-21	زين البحرين	إلزامية	الهيئة العامة لتنظيم قطاع الاتصالات
	2-فبراير-21	زين الكويت	طوعية	DNV-GL
	15-يناير-20	زين الأردن	طوعية	اس جي اس
	5-أبريل-18	زين السودان	طوعية	DNV-GL
نظام إدارة استمرارية الأعمال أيزو 22301:2012	فبراير-20 28-يناير-20	زين الكويت	طوعية	DNV-GL
نظام الإدارة البيئية ايزو 14001:2015	03-فبراير-21	زين الكويت	طوعية	DNV-GL
نظام إدارة الجودة ايزو 9001:2015	16-أبريل-18	زين السودان	طوعية	DNV-GL
	03-فبراير-21	زين الكويت	طوعية	DNV-GL
	15-يناير-21	زين البحرين	طوعية	DNV-GL