إدارة المخاطر

تتكيف زين باستمرار مع التطورات التكنولوجية السريعة مع التأكد كذلك من تبنيها إطاراً قوياً وملائماً ومرناً لإدارة المخاطر، بهدف معالجة المخاطر الحالية والمحتملة..، وتضطلع إدارة المخاطر المؤسسية (ERM) بالمسؤولية عن تحديد المخاطر المحتملة وتقييمها وتحديد أولوياتها وإدارتها، كما تتخذ نهجاً استباقياً للتخفيف من المخاطر، واتخاذ القرارات الاستراتيجية ذات الصلة، من الأمثلة على ذلك تقييم ضوابط أمن المعلومات المعمول بها، التي تعالج التهديدات الأمنية التي تتطور بصفة مستمرة سريعة الوتيرة.

تقدم إدارة المخاطر المؤسسية تقاريرها مباشرة إلى لجنة المخاطر التابعة لمجلس الإدارة (BRC)، التي تشرف بدورها على الالتزام بسياسات وإجراءات إدارة المخاطر وفعالية إطار عمل إدارة المخاطر، وتقوم لجنة إدارة المخاطر بمراجعة الإطار والموافقة عليه على أساس سنوي، بينما يتم مراجعة اتجاهات المخاطر على أساس ربع سنوي، وتساعد الوظائف الأخرى مثل إدارات التدقيق الداخلي وحوكمة الشركات، ولجان مجلس الإدارة التابعة لها، إلى جانب إدارة المخاطر للمجموعة، مجلس إدارة المخاطر في الإشراف عليها.أعلى النموذج

تقوم إدارة المخاطر المؤسسية - بما يتماشى بشكل وثيق مع استراتيجية الاستدامة المؤسسية للشركة - بتقييم الآثار الاجتماعية والاقتصادية والبيئية وحقوق الإنسان للشركة من وجهة نظر المخاطر، وذلك من خلال البحث الاستباقي والمشاركة المكثفة مع أصحاب المصلحة، ومنذ العام 2019، كانت الاعتبارات الرئيسية هي المخاطر والفرص المرتبطة بتغير المناخ وتأثيرها المادي، مما يسمح بالتخطيط في المراحل المبكرة لاستراتيجيات التخفيف من تلك المخاطر عبر الأسواق التشغيلية لـ زين.

تم إدراج شرح متعمق للمخاطر والفرص المتصلة بالمناخ ضمن تقرير فرقة العمل المعنية بالإفصاحات المالية المتصلة بالمناخ في الصفحة **105**.

جمعيات العضوية من منظور المخاطر

تتمتع مجموعة زين بالعديد من العضويات في الجمعيات العالمية التي تضمن توافق الشركة مع معايير الصناعة وأفضل الممارسات العالمية، بما في ذلك:

- اتحاد الـ GSMA، وهي منظمة عالمية تعمل على توحيد منظومة الهواتف النقالة لاكتشاف وتطوير وتقديم الابتكارات الأساسية لبيئات الأعمال الإيجابية والتغيير المجتمعي.
- الاتحاد الدولي للاتصالات ITU، هو وكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات لتسهيل التوصيلية الدولية في شبكات الاتصالات، وتخصيص الطيف الخلوي على الصعيد العالمي، ووضع المعايير التقنية التي تضمن التوصيل البيني السلس للشبكات والتكنولوجيات، وتحسين النفاذ إلى تكنولوجيا المعلومات والاتصالات للمجتمعات المحرومة من الخدمات في جميع أنحاء العالم.
- تشارك مجموعة زين في المؤتمر العالمي للهوافت سنوياً، وتشارك معلومات الصناعة مع أقرانها فيما يتعلق بالترابط والأمن.

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

تواصل زين استخدام مصفوفة التأثير والاحتمالية لتحديد تصنيف المخاطر للأحداث التي تواجه الشركة عبر عملياتها، ويتم تقييم التأثيرات عبر معايير متعددة تشمل المالية والسمعة وتغير المناخ والأسواق والعملاء والموظفين وغيرها، كما يأخذ التصنيف في الاعتبار حالة "ما قبل" و "ما بعد" تخفيف المخاطر، مما يوفر معلومات عن حالة المخاطر المتأصلة والمتبقية للشركة.

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

المبدأ التحوطي

عندما تقوم زين بتصميم منتجاتها وتقديم الخدمات، كمبدأ وقائي، يتم أخذ جميع المتطلبات البيئية المعمول بها في الاعتبار، إذ تركز أعمال زين على تطوير وتقديم منتجات وخدمات منخفضة الكربون حيث يحتاج العملاء إلى التوافق مع طموح الشركة في تحقيق صافي الانبعاثات الصفري، بينما تمثل الاعتبارات المتعلقة بالمناخ مثل استخدام الطاقة وتفكيك المعدات منتهية الصلاحية بغرض الإصلاح أو إعادة الاستخدام بعض التوافقات الرئيسية المدرجة في قائمة المراجعة عندما يتعلق الأمر بتصميم المنتجات والخدمات.

تعمل فرق تصميم المنتجات والمشتريات 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، من خلال هذه المشاركات، تقوم لجنة المخاطر التابعة لمجلس الإدارة، ولجنة العمل المناخي، ومجلس الإدارة بمراقبة المخاطر الرئيسية مثل التقدم السريع في التكنولوجيا.

حماية البيانات والخصوصية

تعتبر زين خصوصية البيانات جزءاً مهماً من الضوابط لتجنب تسرب البيانات، من أجل الامتثال للهيئات الإدارية القانونية والتنظيمية ومتطلباتها، وتحترم زين بشكل كبير خصوصية معلومات التعريف الشخصية (PII) المعهود بها إليها من قبل عملائها وموظفيها ومورديها وأصحاب المصلحة الآخرين، والعمليات التي ينطوي عليها جمع هذه المعلومات واستخدامها والاحتفاظ بها، وعدم الكشف عنها.

في العام 2023، وضعت زين سياسة جديدة لحماية البيانات والخصوصية لضمان استمرارها في تلبية أعلى معايير حماية البيانات والخصوصية لجميع أصحاب المصلحة، وتمت الموافقة عليها من قبل مجلس الإدارة، تضمن هذه السياسة بقاء زين متوافقة مع كافة قوانين ولوائح حماية البيانات والخصوصية ذات الصلة، وتغطي السياسة المحدثة كذلك مجموعة من الموضوعات التي تشمل كيفية قيام الشركة بجمع البيانات الشخصية وإدراتها وتخزينها وحقوق الأفراد في الوصول إلى بياناتهم الشخصية، والتحكم فيها.

يمكن الاطلاع على هذه السياسة عبر الرابط أدناه:

هنا

السياسات والممارسات المتعلقة بجمع وإدارة والاحتفاظ بمعلومات العملاء ومعلومات التعريف الشخصية لكل شركة تعمل في زين:

زين البحرين

يرجى الرجوع إلى الرابط أدناه لمزيد من التفاصيل:

https://www.bh.zain.com/en/copyright/privacy-policy

زين العراق

نفذت زين العراق العديد من الضوابط الأمنية وتتبع أفضل الممارسات لضمان أن جميع البيانات التي تتم معالجتها آمنة، في العام 2023، حصلت زين على شهادة ISO 27001، مما يوفر مزيداً من التأكيد على الضوابط المطبقة لحماية البيانات.

زين الأردن

تم إطلاق قانون جديد لحماية البيانات وتم إجراء تحليل من قبل الفريق القانوني والتنظيمي لعقد ورش عمل مع جميع الأطراف المعنية لتقييم مخاطر بيانات معلومات تحديد الهوية الشخصية ووضع السياسات والإجراءات التصحيحية وفقا لذلك.

زين الكويت

تنطبق لائحة حماية خصوصية البيانات الخاصة بالهيئة العامة للاتصالات وتقنية المعلومات على كل من القطاعين العام والخاص اللذين يجمعان ويعالجان ويخزنان معلومات تحديد الهوية الشخصية، حيث عينت زين مسؤولًا عن خصوصية البيانات، وهو المسؤول عن الإشراف على الضوابط الفنية والتنظيمية المناسبة للامتثال للوائح.

زين السعودية

لدى زين سياسة خصوصية البيانات التي وضعتها ووافقت عليها الهيئة السعودية للبيانات الذكاء الاصطناعي (السلطة المنظمة).

زين السودان

تضمن زين حماية معلومات العملاء ومعلومات تحديد الهوية الشخصية من خلال سياسات مثل مدونة قواعد السلوك الخاصة بها.

زين جنوب السودان

تعمل زين باستمرار على تعزيز ضوابطها الأمنية لتحسين نضجها الأمني والدفاع ضد التهديدات وحماية البيانات من هذه التهديدات، يتم إجراء العديد من تقييمات الرقابة الأمنية لتحديد التحسينات المحتملة التي يمكن تنفيذها.

معلومات العميل لأغراض ثانوية

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

يمكن العثور على مزيد من المعلومات حول حوكمة وسياسات خصوصية البيانات في زين في قسم "منتجاتنا وعملائنا" في الصفحة 64.

حتى العام 2023، لم تكن هناك تقارير أو شكاوى من أطراف ثالثة خارجية وهيئات تنظيمية، أو تحديد تسريبات أو فقدان بيانات عملاء.

أمن البيانات

واصلت زين التزامها بحماية موظفيها وعملائها من هجمات التصيد الاحتيالي، حيث قدمت الشركة نظام إبلاغ سهل الاستخدام، مما يسمح للأفراد بالإبلاغ عن مثل هذه الهجمات ورسائل البريد الإلكتروني غير المرغوب فيها بنقرة بسيطة، تعمل هذه المبادرة على تبسيط عملية التحقيق، وتعزيز الكفاءة التشغيلية بشكل كبير، وتمكين التنفيذ الفوري للإجراءات التصحيحية.

نهج الإدارة لتحديد ومعالجة مخاطر أمن البيانات

تقوم زين بتخزين ومعالجة المعلومات السرية للغاية التي يمكن أن تكون ذات قيمة كبيرة في أيدي مجرمي الإنترنت، وهذا هو السبب في اعتبار البنية التحتية للشركة ذات أهمية حرجة للغاية، يتطور مشهد التهديدات باستمرار، الأمر الذي يتطلب تعزيزاً مستمراً وصارماً للضوابط الأمنية.

لدى زين الضوابط والعمليات الأمنية اللازمة بما يتماشى مع أفضل الممارسات للتخفيف والحد من إمكانية وتأثير الهجمات السيبرانية، وطورت الشركة المرونة السيبرانية، وهي القدرة على تحديد تهديدات الأمن السيبراني الكارثية المحتملة وحمايتها واكتشافها والاستجابة لها والتعافي منها بشكل فعال، ولضمان بيئة آمنة، تقوم زين بحماية بنيتها التحتية من خلال السياسات والإجراءات اللازمة وأنشطة المراقبة المستمرة للدفاع ضد التهديدات.

فيما يلي توضيح لإطار عمل مشار إليه في استراتيجية زين للمرونة الإلكترونية.

التحديد
- ناقلات التهديد والأصول والبيانات والجهات الفاعلة
- التحقق من الصحة مع دراسات تقييم المخاطر ومراقبة البنية التحتية

الحماية
- تثبيت ضوابط التكنولوجيا، حلول النقاط
- تقوية الأنظمة والأجهزة
- آليات التحكم في الدخول

الكشف
- مراقبة البنية التحتية
- التحليلات والبحث عن التهديدات
- الاشتراكات الخارجية

الاستجابة
- خطط إعادة تنظيم وإدارة الحوادث

الاستعادة
- المرونة للاستئناف من "الحالة الطبيعية" في أقرب وقت ممكن
- برونوكولات إدارة الأزمات

فيما يلي بعض الأمثلة على مبادرات الأمن السيبراني في أسواق زين:

- تقييم الأمن السيبراني / نقاط الضعف
- اختبار الاختراق
- تقييم أمن إشارات الاتصالات
- الإبلاغ عن جميع الحوادث والاختراقات الأمنية إلى هيئة الاتصالات
- شهادة نظام إدارة أمن معلومات ISO 27001
- تدريب أمن المعلومات لجميع الموظفين

إدارة المخاطر النظامية الناجمة عن الاضطرابات التكنولوجية

تتطلب الخدمات الحيوية للمهام توافرا مستمرا عندما تكون فترات انقطاع الخدمة غير محتملة، ويمكن أن تؤدي إلى أضرار فورية وكبيرة، وتراقب زين أي اضطرابات تحدث في جميع أنظمتها الرئيسية.

وصف الأنظمة لتقديم الخدمة دون عوائق أثناء وجود انقطاعات

الـ **Core:** يشمل PS Core و CS Core (المذكور سابقا في تقارير زين السابقة للاستدامة).

CS Core: Circuit Switch، و الخاص بالتعامل مع المكالمات الصوتية ووظائف الاحتواء مثل تبديل الهاتف النقال (MSC) Center، وبوابة MSC (GMSC).

PS Core: Packet Switch، و الخاص بالتعامل مع جلسات البيانات ووظائف الاحتواء مثل: عقدة دعم S+H9erving GPRS (SGSN)، وعقدة دعم بوابة GPRS (GGSN)، وخادم اسم المجال (DNS)، وخادم بروتوكول التكوين الديناميكي للمضيف (DHCP)، وبوابة شحن الحزم، إلخ.

الشحن: إريكسون - نظام للعملاء لإعادة شحن حساباتهم بالائتمان والحفاظ على معلومات الرصيد، تستخدم من قبل عملاء الدفع المسبق والدفع الآجل.

مجموعة زين

نظام	توافر
تخطيط موارد المؤسسات	100%
أوراكل هايبريون	100%
موقع مجموعة زين	100%

زين البحرين

نظام	توافر
Core	100%
شحن	100%
الموقع الإلكتروني	100%

زين العراق

نظام	توافر
Core	100%
شحن	100%
الموقع الإلكتروني	100%

زين الأردن

نظام	توافر
Core	99.96%
شحن	100%
الموقع الإلكتروني	99.99%

زين الكويت

نظام	توافر
Core	99.95%
شحن	99.95%
الموقع الإلكتروني	100%

زين السعودية

نظام	توافر
Core	99.99%
شحن	100%
الموقع الإلكتروني	100%

زين جنوب السودان

نظام	توافر
Core	100%
شحن	99.8%
الموقع الإلكتروني	غير متاح

زين السودان

نظام	توافر
Core	100%
شحن	100%
الموقع الإلكتروني	100%

التدريب على المخاطر الأمنية

تعد عمليات التدريب والتوعية المستمرة مطلوبة للدفاع ضد التهديدات التي تتطور بوتيرة سريعة، كجزء من برنامج زين للتوعية بالأمن السيبراني تحت عنوان قف.فكر.تصرف، إذ تعمل الشركة على زيادة الوعي فيما يتعلق بما يجب وما لا يجب فعله في أمن المعلومات وكذلك كيفية الإبلاغ عن الأنشطة المشبوهة.

بالإضافة إلى ذلك، تدرك زين أن معلومات التهديدات تلعب دورا حاسما في الدفاع ضد التهديدات المتنامية، وتواصل اشتراكاتها في الإشعارات والتنبيهات التي يتم إنشاؤها من منصة مشاركة معلومات البرمجيات الخبيثة التابعة لمركز تحليل مشاركة معلومات الاتصالات التابع لاتحاد الـ "جي إس إم إيه"، وتساعد هذه التنبيهات زين على التزود بالاستباقية في اتخاذ الخطوات الدفاعية اللازمة في الوقت المناسب لصد الهجمات السيبرانية.

موضوعات أمن المعلومات التي تم التخطيط لها وتغطيتها في العام 2023

- إنشاء كلمات مرور قوية - تدريب على الوعي الأمني
- الروابط والمرفقات: فكر قبل النقر
- 2023 تحذيرات الهندسة الاجتماعية
- الاحتيال الإلكتروني: لا تقع في الفخ
- فهم عناوين URL
- طريقة Kevin Mitnick - هجوم المصادقة الثنائية
- التهديدات الشائعة للعام 2023
- تهديدات الفدية الرقمية
- الروابط والمرفقات: فكر قبل النقر
- وسائل التواصل الاجتماعي: البقاء آمنا في عالم متصل
- رموز QR: المسح الآمن
- أفضل ممارسات أمان البريد الإلكتروني!
- دروس زين البحرين: مفتاح مرونة الأمن السيبراني
- سياسة وسائل التواصل الاجتماعي
- إدارة الأجهزة النقالة
- اللائحة العامة لحماية البيانات والامتثال لها
- الوعي بالأنشطة الاحتيالية غير المرغوب فيها
- أمن الهاتف
- إجراءات أمن الموقع
- الاحتيال والتصيد
- أمن المعلومات
- الاتصال اللاسلكي
- أمن كلمة المرور
- تصفح آمن للإنترنت
- الوعي بالسياسات
- الهندسة الاجتماعية
- الأمن المادي
- منع الاحتيال

تحديثات التوعية لعام 2023

	الكويت	السعودية	البحرين	العراق	الأردن	السودان	جنوب السودان
مجموع الموظفين	1,773	1,798	385	912	1,186	788	145
إجمالي عدد الموظفين الذين تلقوا محتوى توعويا	1,773	1,798	385	912	1,186	788	145
إجمالي عدد القنوات المستخدمة	5	1	4	1	1	2	3
القنوات المستخدمة	تاقصلم تاتفلا البريد الإلكتروني للشركات النشرة الإخبارية الرسائل التعريفية القصيرة	جلسة توعية بالتصيد والاحتيال، رسائل البريد الإلكتروني، شاشة عرض الاجتماعات الفعلية	النشرة الإخبارية للشركات عبر البريد الإلكتروني صفحة الشاشة جلسات مباشرة منصة التوعية	البريد الإلكتروني للشركات النشرة الإخبارية شاشات التوقف التعريفي جلسة التوعية	البريد الإلكتروني للشركة والنشرة الإخبارية ومقاطع الفيديو والجلسات وجهًا لوجه وتمارين التصيد الاحتيالي	التعريف بواسطة النشرة الإخبارية للشركات عبر البريد الإلكتروني وسائل التواصل الاجتماعي	النشرة الإخبارية للشركات عبر البريد الإلكتروني تطبيق واتس أب الرسائل القصيرة الجلسات البدنية

تتكون القائمة التالية من الدورات التدريبية للأمن السيبراني التي يتلقاها موظفو إدارة المخاطر في جميع عمليات زين.

- أخصائي معتمد في المخاطر والامتثال
- معتمد في مراقبة المخاطر ونظم المعلومات
- ISO22301 كبير المدققين
- COBIT
- إدارة العمليات الأمنية
- إدارة الأمن السيبراني

المبادرات مع أصحاب المصلحة الخارجيين

مبادره	تاريخ الاعتماد	الشركات العاملة في النطاق	طبيعة المبادرة (ملزمة/طوعية)	مجموعة من أصحاب المصلحة المعنيين
نظام إدارة أمن المعلومات ISO 27001:2013	10 - يناير - 21	زين البحرين	إلزامي	هيئة تنظيم الاتصالات
	07 - يناير - 23	زين العراق	تطوعي	AQC
	2 - فبراير - 21	زين الكويت	تطوعي	DNV-GL
	15 - يناير - 20	زين الأردن	تطوعي	اس جي اس
	11 - أبريل - 21	زين السودان	تطوعي	DNV-GL
نظام إدارة استمرارية الأعمال ISO 22301:2012	20 - فبراير 28 - يناير - 20 29 - يناير - 23	زين الكويت	تطوعي	DNV-GL
نظام الإدارة البيئية ISO 14001:2015	3 - فبراير - 21	زين الكويت	تطوعي	DNV-GL
نظام إدارة الجودة ISO 9001:2015	3 - فبراير - 21	زين الكويت	تطوعي	DNV-GL
	15 - يناير - 21	زين البحرين	تطوعي	DNV-GL
IT Service Management System ISO 20000-1	31 - يناير - 23	زين الكويت	تطوعي	DNV-GL