أمن المعلومات

عزز البنك التزامه خلال عام 2025م بالحفاظ على أعلى مستويات الثقة والمرونة التشغيلية عبر تحويل نهجه الأمني من الأسلوب التفاعلي إلى نهج استباقي شامل قائم على المخاطر والاستفادة من تحليلات التهديدات السيبرانية، بما يعزز الحوكمة والالتزام التنظيمي ويضمن استمرارية الأعمال دون انقطاع.

أبرز إنجازات 2025م

100% نسبة معالجة الحوادث الأمنية ضمن اتفاقية مستوى الخدمة **(SLA)** مع الحفاظ على استقرار أداء الاستجابة للحوادث.

رفع فاعلية مراجعات البنية المعمارية الأمنية، مما أسهم في خفض ملحوظ للملاحظات عالية المخاطر في الأنظمة الحيوية.

100% نسبة إنجاز كافة برامج التوعية الأمنية المجدولة للموظفين والعملاء.

100% نسبة الالتزام بمتطلبات الأمن مع عدم وجود أي ملاحظات جوهرية في تقييمات أمن واجهة برمجة تطبيقات المصرفية المفتوحة **(Open Banking API)**.

الحصول على النسخة الرابعة من شهادة الاعتماد في الامتثال لمعايير أمن البيانات الخاصة ببطاقات الدفع مع المواءمة الكاملة لمتطلبات إطار الأمن السيبراني الصادر عن البنك المركزي السعودي ومتطلبات الهيئة الوطنية للأمن السيبراني.

التحول الاستراتيجي والتميز في الأداء

تركز التنفيذ الاستراتيجي للبنك على تحقيق تحسينات ملموسة في فاعلية الرقابة، حيث شملت المبادرات الرئيسية ما يلي:

الدفاع الاستباقي

عزز البنك الموقف الأمني من خلال تحسينات الكشف في الوقت الفعلي (نضج مركز العمليات الأمنية وتحسين كشف التهديدات، وتحديثات منظومة SIEM)، مِمّا اقترن بزيادة الأتمتة والمراقبة الناتجة من تحليلات التهديدات السيبرانية.

الالتزام التنظيمي

حقق البنك المواءمة الكاملة مع معايير إطار الأمن السيبراني الصادر عن البنك المركزي السعودي (SAMA CSF) ومعايير الهيئة الوطنية للأمن السيبراني، كما أتم الحصول على شهادة PCI DSS v4.0، مع استمرار تتبع الجاهزية لمتطلبات البنك المركزي لضمان أعلى مستويات الالتزام.

المرونة التشغيلية

حافظ أداء الاستجابة للحوادث على استقراره العالي، حيث بلغت نسبة معالجة كافة الحوادث المكتشفة ضمن اتفاقيات مستوى الخدمة (SLAs) 100%.

عزز البنك بشكل جوهري خلال عام 2025م حوكمة الأمن السيبراني للأطراف الخارجية وعمليات تقييم المخاطر والالتزام عبر إدراج تدابير العناية الواجبة المستمرة، ويساهم هذا النهج الاستباقي في توسيع النطاق الأمني للبنك وتعزيز المرونة الكلية للنظام.

الحوكمة والمخاطر والالتزام (GRC)

يواصل البنك تعزيز هياكل الحوكمة لضمان أمن العمليات وامتثالها، لا سيما في المجالات الحيوية مثل المصرفية المفتوحة والبيئات السحابية.

البنية المعمارية الآمنة

تطوير مسار البنية المعمارية الآمنة، بما عزّز حوكمة التصميم وأدى إلى خفض القضايا عالية المخاطر. كما تحسّن مستوى الالتزام عبر دمج مراجعات البنية المعمارية ضمن جميع الأنظمة الرئيسية.

أمن واجهات برمجة التطبيقات والمصرفية المفتوحة

أجرى البنك تقييماً واختباراً لضوابط أمن واجهات برمجة التطبيقات عبر بوابتها المخصصة والواجهات الخاصة بالمصرفية المفتوحة تماشياً مع معايير البنك المركزي السعودي المحدثة، حيث أكدت عمليات فحص الثغرات واختبارات الاختراق والمراقبة المستمرة تحقيق نسبة امتثال بلغت 100% دون وجود أي ملاحظات جوهرية، مِمّا يضمن استمرارية عمليات المصرفية المفتوحة بأمان ومرونة وموثوقية تنظيمية تامة.

الجاهزية السيبرانية والمرونة

طور البنك برامج محاكاة الهجمات السيبرانية لتعزيز المرونة التشغيلية عبر توسيع نطاق حوكمة أمن السحابة وتقوي ضوابط أمن البيانات، بما يتوافق مع متطلبات البنك المركزي السعودي والهيئة الوطنية للأمن السيبراني.

ثقافة الأمن والتركيز على العملاء

يؤمن البنك بأن الأمن مسؤولية جماعية، ومن هذا المنطلق يحرص على إشراك السفراء والعملاء بفاعلية في بناء ثقافة أمنية متينة.

برامج التوعية

حقق البنك نسبة إنجاز بلغت 100% لكافة برامج التوعية الأمنية المجدولة المقدمة للسفراء والعملاء، إذ شملت هذه البرامج حملات عبر البريد الإلكتروني، ومنشورات على الشبكة الداخلية، وورش عمل، بالإضافة إلى نصائح أمنية خارجية موجهة للعملاء.

الأمن الموجه للعملاء

ساهمت مرئيات العملاء بشكل مباشر في تطوير العديد من التحسينات على البروتوكولات الأمنية، مِمّا يهدف إلى تحقيق التوازن بين الحماية القوية والتجارب الرقمية السلسة. شملت هذه التحسينات ما يلي:

- تبسيط إجراءات المصادقة متعددة العوامل (MFA) عبر دمج الأجهزة الموثوقة وخيارات البصمة الحيوية.
- تقليل حالات انتهاء صلاحية الجلسة (Session time-out) مع الحفاظ على مستويات الأمان.
- تحسين واجهة المستخدم للتنبيهات الأمنية لضمان استيعاب العملاء لها بشكل أفضل.
- تعزيز مبادرات التواصل والتوعية الموجهة للعملاء عبر القنوات الرقمية.