تعزيز التقنية المالية:

مخطط على مستوى مجلس الإدارة لإعطاء الأولوية للدفاع السيبراني

الجزء الأول - تحديد أولويات الأمن السيبراني لقادة التقنية المالية غير التقنيين

الملخص:

حيث أن المنطقة تشهد نمو متزايد في مجال التقنية المالية، إلا أن الجرائم السيبرانية لا تزال تشكل مخاوف بالنسبة لمجالس الإدارة في القطاع المالي. ولكسب الثقة في استخدام التقنية المالية فإن ذلك يعتمد بشكل كبير على قدرة مقدمي الحلول التقنية والأمنية على صد الهجمات السيبرانية وحماية بيانات المستخدمين بكفاءة.
وقد أدت حالات اختراق التقنية المالية الأخيرة مثل الهجوم السيبراني على شركة التقنية المالية (Lykke) في يونيو 2024[1] واختراق شركة التقنية المالية ريفولوت (Revolut) في يوليو 2023[2] إلى زعزعة ثقة أصحاب المصلحة.

هذه المقالة هي الأولى في سلسلة الريادة الفكرية المكونة من أربعة أجزاء من بي دبليو سي، والتي تقدم رؤى عملية لقادة التقنية المالية حول المجالات التقنية الأساسية لإعطائها الأولوية في الحماية والأمن السيبراني حيث تم إنشاء تصميم البنية الأساسية للتقنية المالية والتحقق منه بناءً على تحليل آلية عملية الدفع عن طريق المحفظة الرقمية. كما تم إجراء تحليل موضوعي للتصميم الهيكلي الأساسي لاستخلاص ثلاث مجالات محورية أساسية للأمن السيبراني فيما يتعلق بالتقنية المالية. يعتقد المؤلف أنه لا بد أن يكون هنالك إشرافًا مستمرًا من مجلس الإدارة للحصول على ضمان سيبراني مستدام، وتخفيف المخاطر، وتعزيز الثقة في التقنية المالية.

المقدمة:

من المتوقع أن يشهد قطاع التقنية المالية في منطقة الشرق الأوسط وشمال أفريقيا نموًا قويًا، وذلك استنادًا إلى خطة التحول الوطني الواعدة، والبيئة التنظيمية القوية، ووجود الكوادر الشابة والطموحة. ومن المتوقع كذلك أن يصل حجم سوق التقنية المالية في منطقة الشرق الأوسط وشمال أفريقيا إلى 1.51 مليار دولار أمريكي في عام 2024، و2.40 مليار دولار أمريكي بحلول عام 2029، مع نمو سنوي بنسبة 9.71٪.[3]

ومع الطموحات الحكومية الكبيرة ولا سيما في مجال التقنية المالية، فإن خارطة النمو تنبع من المبادرات الموزعة استراتيجيًا في مختلف المراكز المالية في المنطقة. حيث تتراوح هذه المبادرات من سوق أبوظبي العالمي وخليج البحرين للتكنولوجيا المالية إلى فنتك السعودية ومركز دبي المالي العالمي للتكنولوجيا المالية.

كما وضعت كل من المملكة العربية السعودية ومملكة البحرين ودولة قطر والإمارات العربية المتحدة استراتيجيات وطنية للتقنية المالية، بالإضافة إلى توفير المزيد من الدعم المادي لقطاع التقنية المالية من خلال المسرعات والحاضنات التي ترعاها الحكومات مثل البيئات التجريبية التنظيمية.

[1] https://www.lykke.com/incident-updates/faq
[2] https://www.bloomberg.com/news/articles/2023-07-09/thieves-stole-20-million-via-revolut-us-payment-flaw-ft-says
[3] https://www.mordorintelligence.com/industry-reports/mena-fintech-market

تعزيز الثقة في التقنية المالية: الدور المحوري للأمن السيبراني

لدى المستخدمين دور رئيسي في نمو التقنية المالية في منطقة الشرق الأوسط وشمال إفريقيا. حيث أن زيادة اعتماد المستخدمين على التقنية المالية في تعاملاتهم المالية، يساهم بشكل كبير في توسع نطاق نمو شركات التقنية المالية، وذلك بالاعتماد على بنية تحتية قائمة على الإنترنت والاتصال عبر الهواتف المحمولة.

ومع ذلك فإن مسار نمو التقنية المالية في منطقة الشرق الأوسط وشمال أفريقيا ليس خالياً من العوائق. فما زال أغلب سكان المنطقة، بما يصل إلى 83%، يتبعون الأساليب التقليدية في إدارة الأموال، وذلك بالاعتماد على الأنظمة المصرفية القديمة.[4]

وعليه فإن تعزيز الثقة في التقنية المالية يتطلب تحولاً جذرياً في سلوك المستخدمين، ما يدفعهم إلى التحول من الخدمات المصرفية التقليدية إلى بدائل التقنية المالية الأكثر حداثة. وتستند الثقة في التقنية المالية على عدة ركائز، تتمثل في: قيمة العلامة التجارية، والامتثال التنظيمي، وشفافية نظام الفوترة، والشراكات/الاتفاقيات مع الهيئات المالية العالمية، والاستقرار المالي، وخصوصية البيانات. أكبر المخاوف وأكثرها إلحاحًا كانت ولا تزال متعلقة **بالأمن السيبراني.**

ويتضح ذلك من أثر الجرائم السيبرانية سلبًا على الثقة في قطاع التقنية المالية، حيث أن هنالك علاقة عكسية بين ازدياد حالات الاحتيال الإلكتروني وثقة المستخدمين في هذا القطاع. ويتناول تقرير بي دبليو سي الحوادث السيبرانية الأخيرة في قطاع التقنية المالية والتي هزت ثقة السوق في هذا القطاع.

إن المشهد المتطور باستمرار للجرائم السيبرانية يستوجب الإشراف على مستوى مجلس الإدارة في سياق استدامة الأعمال، بدلاً من اعتباره مجرد استجابة تنظيمية لاحقة. إن نهج شركات التقنية المالية الذي يضع التقنية في المقام الأول في إدارة الأموال، يعني أن استراتيجية الأمن السيبراني القوية تتمثل في ضرورة الحوكمة الواضحة والمساءلة على مستوى مجلس الإدارة.

وضع مخطط على مستوى مجلس الإدارة لتحديد أولويات الدفاع السيبراني

لقد واجهت مجالس الإدارة و مستثمري رأس المال (VCs) والقادة التنفيذيون صعوبات في قياس تأثير الأمن السيبراني على الأعمال التجارية. ولذلك يعتمد مسؤولو أمن المعلومات على مؤشرات لتقييم الأثر منها العائد على الاستثمار في الأمن، والامتثال للأطر التنظيمية الصادرة عن الجهات التنظيمية مثل هيئة البيانات والذكاء الاصطناعي السعودية، والبنك المركزي السعودي، والبنك المركزي لدولة الإمارات العربية المتحدة؛ وذلك لعكس دور الأمن السيبراني على لغة الأعمال.

إن مجالس إدارة شركات التقنية المالية قادرة على بذل المزيد من الجهود لتعزيز رقابتها واشرافها. حيث أن المراجعات الفنية المتعمقة قد تشكل استجابة غير مناسبة، الأمر الذي يحتم معه على مجالس الإدارة أن تختار نهجاً يتسم بالأولوية ـ نهج يستعرض عناصر الصمود السيبراني تبعًا لأهميتها.

[4] https://www.imf.org/en/Publications/fandd/issues/2023/09/unleashing-mideast-fintech-amjad-ahmad#:~:text=Still%2C%20only%2017%20percent%20of,percent%20in%20the%20United%20States.

تصور بنية أساسية للتقنية المالية

على الرغم من أن حلول التقنية المالية ليست متشابهة، وأن كل مزود للحلول يعمل انطلاقًا من بنية فريدة تضم واجهات المستخدم ومنطق الأعمال والقدرات، فإن البنية الأساسية التي تحدد العناصر الأساسية ضرورية لفهم وظائف التقنية المالية.

يمكن تقسيم معظم حلول التقنية المالية إلى ثلاث مستويات رئيسية:

01

مستوى المستخدم: يشمل المستخدم النهائي الذي يتفاعل مع حلول التقنية المالية من خلال تطبيق الهاتف المحمول أو المتصفح.

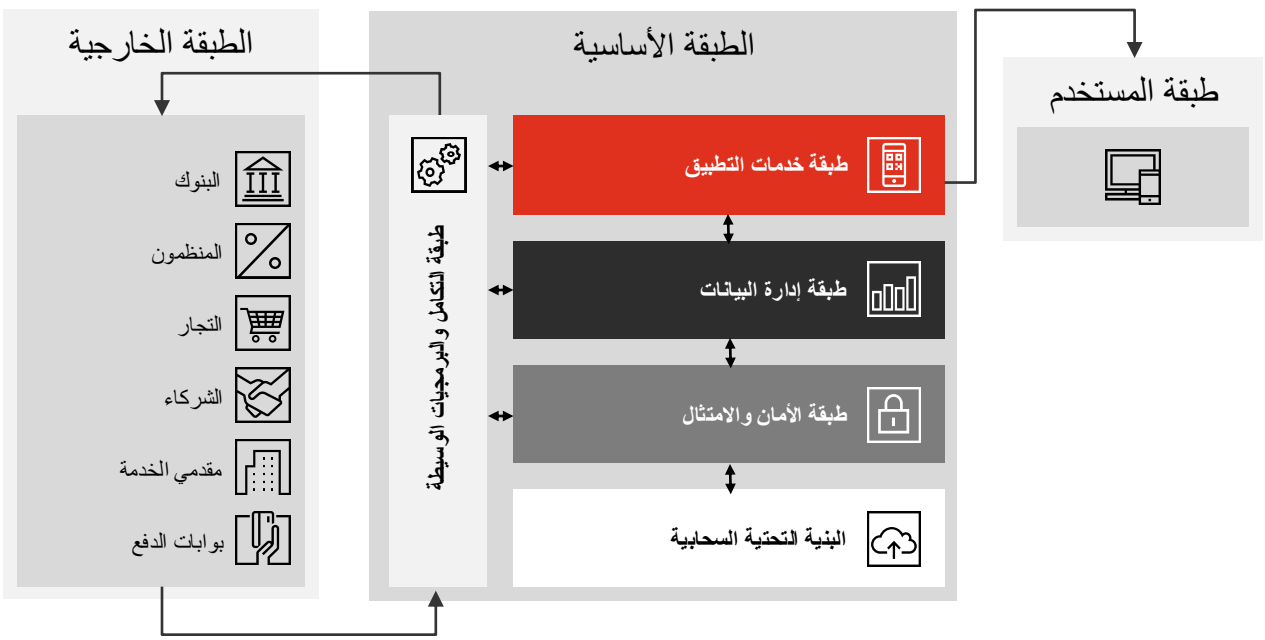
02

المستوى الأساسي: يشمل الحل التقني المالي بما في ذلك المنطق التجاري، قاعدة البيانات، البنية التحتية السحابية، ووسيط البرمجيات.

03

المستوى الخارجي: يشمل الأطراف الخارجية مثل البنوك والهيئات التنظيمية التي يتكامل معها الحل التقني المالي.

يتم توضيح المستويات الرئيسية للحلول التقنية المالية وتدفقات بيانات المستخدم المرتبطة بها في الشكل 1.1.



الشكل 1.1: تصور المستويات الرئيسية للتقنية المالية

تم وصف المستويات الرئيسية للتقنية المالية في الجدول 1.1

الوصف	المكونات
مستوى المستخدم: يهدف مستوى المستخدم إلى توفير واجهة آمنة، سريعة الاستجابة، وسهلة الاستخدام تلبي احتياجات العملاء مع ضمان اتصال سلس بالأنظمة الأساسية.	1. **الأجهزة:** يصل المستخدمون إلى خدمات التقنية المالية من خلال أجهزة مثل الهواتف الذكية، الأجهزة اللوحية، وأجهزة الكمبيوتر. 2. **الواجهات:** تطبيقات الهاتف المحمول، البوابات الإلكترونية، أو واجهات المستخدم الأخرى التي تسمح للمستخدمين بالتفاعل مع النظام، تنفيذ المعاملات، والوصول إلى الخدمات. 3. **تجربة المستخدم:** هذه المستوى مهمة لضمان تجربة سلسة وبسيطة لأنها تؤثر مباشرة على رضا المستخدم ومشاركته.
المستوى الأساسي: يشكل المستوى الأساسي العمود الفقري لهندسة التقنية المالية. وهي تحدد المنطق التجاري لحلول التقنية المالية، وتخزن وتدير البيانات، وتشمل مستوى البنية التحتية السحابية، والحلول الأمنية السيبرانية، وواجهات البرمجة (APIs).	1. **مستوى خدمات التطبيقات:** تشمل المنطق التجاري والتطبيقات التي توفر الخدمات المالية مثل المدفوعات، والإقراض، والاستثمارات، والتأمين، إلخ. كما تتضمن إدارة حسابات المستخدمين، ومعالجة المعاملات، إلخ. 2. **مستوى إدارة البيانات:** تتعامل هذه المستوى مع تخزين البيانات ومعالجتها وإدارتها. وتشمل قواعد البيانات، ومخازن البيانات، وتقنيات البيانات الضخمة التي تخزن البيانات الخاصة بالمعاملات، وبيانات المستخدم، والسجلات المالية. كما تعتبر حوكمة البيانات، وخصوصية البيانات، ونزاهة البيانات مكونات أساسية في هذه المستوى. 3. **مستوى الأمن والامتثال:** تشمل هذه المستوى التدابير الأمنية مثل التشفير، والمصادقة، واكتشاف الاحتيال، والتحكم في الوصول. كما تتضمن آليات الامتثال الالتزام بالمتطلبات التنظيمية مثل "اعرف عميلك" (KYC)، ومكافحة غسل الأموال (AML)، ولوائح حماية البيانات مثل قانون حماية البيانات الشخصية في المملكة العربية السعودية (KSA PDPL) وقانون حماية المستهلك في الإمارات العربية المتحدة (UAE CPS) وقانون حماية البيانات في مركز دبي المالي العالمي (DIFC).[5] 4. **البنية التحتية السحابية:** يدعم مكون البنية التحتية نشر المستويات المشار إليها أعلاه في بيئة سحابية، مما يتيح قابلية التوسع، والمرونة، والصمود. قد تشمل البنية التحتية السحابية سحابة عامة أو خاصة أو هجينة، وذلك بحسب المتطلبات المحددة لمنصة التقنية المالية. 5. **مستوى التكامل والبرمجيات الوسيطة:** يعمل هذا المكون كحلقة وصل تربط الأنظمة المختلفة، والخدمات، والجهات الخارجية. مما يسهل التواصل بين كل من التطبيقات المختلفة، والخدمات، والمستويات داخل الهندسة الأساسية ومع الجهات الخارجية. بالإضافة إلى ذلك تشمل مكونات وسيط البرمجيات واجهات برمجة التطبيقات (APIs)، ووسطاء الرسائل، والحافلات الخدمية.

←

[5] https://www.law-middleeast.com/gccs-data-privacy-regulations-decoded/#:~:text=Processing%20personal%20data%20is%20prohibited,whom%20the%20data%20is%20disclosed.

تم وصف المستويات الرئيسية للتقنية المالية في الجدول 1.1

الوصف	المكونات
المستوى الخارجي: يتكون المستوى الخارجي من جهات خارجية تتكامل مع نظام التقنية المالية. حيث أن هذه الجهات ضرورية لتقديم خدمات مالية شاملة في سبيل الحفاظ على الامتثال.	1. **البنوك:** تمكن البنوك من معالجة المدفوعات، الاحتفاظ بأموال العملاء، وتقديم خدمات أخرى مدمجة مع منصة التقنية المالية. 2. **الهيئات التنظيمية:** تشرف الهيئات على الامتثال للمتطلبات القانونية والتنظيمية، مثل سلطات السلوك المالي أو البنوك المركزية. 3. **التجار:** الشركات التي تستخدم منصة التقنية المالية لقبول المدفوعات، تقديم الخدمات، أو التعامل مع العملاء. 4. **الشركاء ومقدمو الخدمات:** البائعون والشركاء الخارجيين الذين يقدمون خدمات إضافية مثل منع الاحتيال، التحليلات، أو طرق الدفع الإضافية. 5. **بوابات الدفع:** بوابات الدفع ضرورية في تمكين معالجة المعاملات بين المستخدمين والتجار، فضلًا عن ضمان تحويل الأموال بشكل آمن في الوقت الفعلي.

دراسة حالة: تلخيص النقاط الرئيسية في الأمن السيبراني للبنية الأساسية للتقنية المالية:

بينما يحتاج كل مكون في البنية الأساسية للتقنية المالية إلى متطلبات الأمن السيبراني المحددة بشكل دقيق، إلا أن هناك عناصر أساسية لدور التقنية المالية تبرر الرقابة المنتظمة على مستوى مجلس الإدارة.

فمثلًا لدينا المحفظة الرقمية – وهي منصة تتيح تخزين وإدارة طرق دفع المعاملات. حيث يُقدر حجم سوق المدفوعات الرقمية في منطقة الشرق الأوسط وشمال أفريقيا بنحو 226.53 مليار دولار في عام 2024، ومن المتوقع أن يصل إلى 380.86 مليار دولار بحلول عام 2029.[6]

STC Pay (المملكة العربية السعودية)، و payit (الإمارات العربية المتحدة)، و ValU (مصر)، و Apple Pay (الولايات المتحدة الأمريكية)، و Google Pay (الولايات المتحدة الأمريكية) تعد امثلة على المحافظ الرقمية التي تمتلك قاعدة مستخدمين واسعة في المنطقة.

ولإيضاح مفهوم ودور البنية الأساسية للتقنية المالية، تتناول الفقرة أدناه تسلسل عملية الدفع عبر المحفظة الرقمية من قبل المستخدم. لنفترض حالة مستخدم يبدأ معاملة دفع من خلال المحفظة الرقمية. سنستعرض البنية الأساسية ونحلل عملية المعاملة بعد ذلك.

[6] https://www.verifiedmarketresearch.com/product/digital-wallets-market/#:~:text=Digital%20Wallets%20Market%20Size%20and,forecasted%20period%202024%20to%202030.

التحقق من صحة البنية الأساسية للتقنية المالية:

من المفيد البدء بالتحقق من صحة البنية الأساسية للتقنية المالية في سياق المحفظة الرقمية. وعليه، أدناه تحليل للمحفظة الرقمية من خلال ربطها بمستويات البنية الأساسية للتقنية المالية.

مستوى المستخدم:

يصل المستخدمون إلى المحافظ الرقمية عبر الهواتف الذكية، والأجهزة اللوحية، والأجهزة القابلة للارتداء (wearables) فعلى سبيل المثال، يتم تضمين Apple Pay في أجهزة iOS مثل Phone او Apple Watch و iPad، بينما يمكن الوصول إلى محفظة Google على أجهزة Android.

المستوى الأساسي:

مستوى خدمات التطبيقات:
معالجة الدفع، والترميز، وإدارة المعاملات هي بعض العمليات التجارية للمحفظة الرقمية التي تُعرّف في مستوى التطبيقات.

مستوى إدارة البيانات:
يتم تخزين بيانات هوية المستخدم، ومعلومات الدفع، وسجلات المعاملات، والبيانات من التطبيقات المتكاملة، من بين أنواع أخرى، بشكل آمن في هذه المستوى.

مستوى الأمان والامتثال:
يتم تطبيق إجراءات الأمن السيبراني مثل التشفير، والتحقق الثنائي من الهوية، والتحقق البيومتري (Biometrics) عبر المحفظة الرقمية. وأما فيما يتعلق بالضوابط الداخلية، فيتم تنفيذ حلول الأمن السيبراني مثل جدران الحماية، ونظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM)،[7] وحلول مكافحة البرمجيات الضارة. كما يتم تطبيق آليات مثل مراقبة المعاملات، وبصمة الأجهزة، وتحديد الموقع الجغرافي لمنع وحظر المعاملات الاحتيالية.

البنية التحتية السحابية:
داخليًا، تعتمد خدمات تطبيق الدفع على البنية التحتية السحابية – مثل خدمات أمازون ويب (AWS)، مايكروسوفت أزور (MS Azure)، وقوقل كلاود (Google Cloud)– لتوفير خدمات مرنة، وقابلة للتوسع، وذات توافر عالي. وذلك بناءً على نموذج الاستعانة بمصادر خارجية مع مقدم خدمات السحابة (CSP)، حيث قد تُبنى المحفظة الرقمية على البنية التحتية كخدمة (IaaS)، أو النظام الأساسي كخدمة (PaaS)، أو البرنامج كخدمة (SaaS) في السحابة. كما يتم تنفيذ خدمات السحابة مثل المحاكاة الافتراضية (Virtualisation)[8] وإدارة السحابة (Cloud Orchestration) في هذا المستوى.

مستوى التكامل والبرمجيات الوسيطة:
يتم ربط المحافظ الرقمية عبر واجهات برمجة التطبيقات (APIs) مع البنوك، وشبكات الدفع، والتجار.

- تتيح واجهات برمجة التطبيقات الخاصة بالبنوك للمحافظ الرقمية إضافة بطاقات جديدة لمشاركة بيانات المعاملات، والمصادقة، وتفويض معاملات المستخدمين.
- تتيح واجهات برمجة التطبيقات لشبكات الدفع من شركات مثل Visa و Mastercard للمحافظ الرقمية معالجة المدفوعات مع التجار وبين المستخدمين.
- تتيح واجهات برمجة التطبيقات الخاصة بالتجار للبائعين قبول المدفوعات من المحفظة الرقمية على مواقعهم الإلكترونية، تطبيقاتهم، أو متاجرهم المادية (physical stores) عبر قارئ البطاقة (نقطة البيع POS).

[7] https://www.microsoft.com/en-us/security/business/security-101/what-is-siem#:~:text=Security%20information%20and%20event%20management,threats%20before%20they%20disrupt%20business.
[8] https://www.redhat.com/en/topics/automation/what-is-cloud-orchestration

التحقق من صحة البنية الأساسية للتقنية المالية:

تتفاعل المحفظة الرقمية مع عدد من الجهات الخارجية:

المستوى الخارجي:

البنوك: ترتبط المحافظ الرقمية بالبنوك عبر واجهات برمجة التطبيقات لربط الحسابات أو البطاقات وتفويض المدفوعات.

شبكات الدفع: تستخدم المحافظ الرقمية واجهات برمجة التطبيقات من شبكات الدفع لمعالجة المعاملات وضمان الامتثال لمعايير الدفع، مما يمكن من معالجة المدفوعات بشكل آمن.

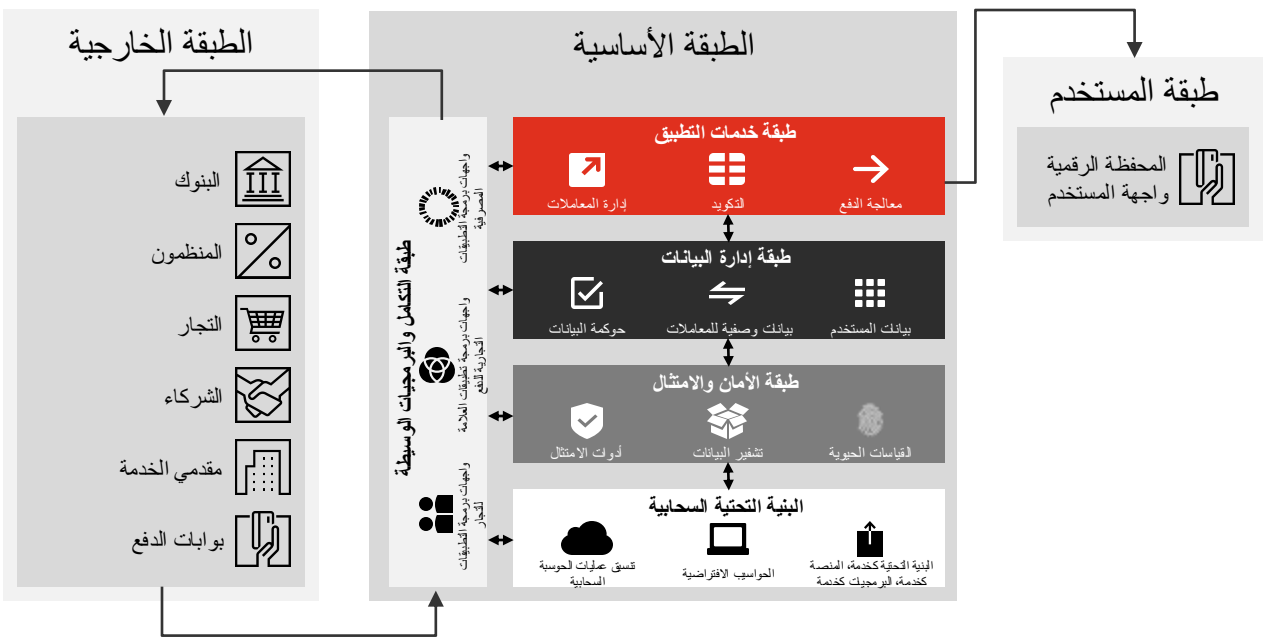
التجار: تتفاعل المحافظ الرقمية مع التجار عبر واجهات برمجة التطبيقات لتسهيل معالجة المدفوعات، وإدارة المعاملات، ودعم أدوات التفاعل مع العملاء.

مقدمو الخدمات: تتكامل المحافظ الرقمية مع مقدمي الخدمات الخارجيين عبر واجهات برمجة التطبيقات لتعزيز اكتشاف الاحتيال، والتحقق من الهوية، وتحليلات المستخدمين.

بوابات الدفع: ترتبط المحافظ الرقمية مع بوابات الدفع عبر واجهات برمجة التطبيقات لمعالجة المعاملات بشكل آمن والتعامل مع تفويضات الدفع.

الجهات التنظيمية: يتم تنفيذ التقارير التنظيمية للهيئات المختصة من خلال واجهات برمجة التطبيقات ذات الصلة.

الشكل 1.2: يمثل ربط المحفظة الرقمية بالبنية الأساسية للتقنية المالية



الشكل 1.2: ربط المحفظة الرقمية بالبنية الأساسية للتقنية المالية

يظهر الربط أن البنية الأساسية للحلول التقنية المالية تدعم بشكل فعال مختلف مكونات المحفظة الرقمية.

تستعرض الخطوة التالية تقييم معمّق لعملية الدفع في سياق البنية الأساسية للحلول التقنية المالية.

تحليل عملية الدفع عبر المحفظة الرقمية بناءً على البنية الأساسية للتقنية المالية:

لنفترض حالة مستخدم يرغب في إجراء الدفع باستخدام المحفظة الرقمية. تتضمن العملية عدة خطوات تمتد عبر مستويات مختلفة من البنية الأساسية لتقنية المالية، وذلك على النحو الآتي:

01

بدء عملية الدفع في مستوى المستخدم:
يقوم المستخدم ببدء الدفع عبر تطبيق المحفظة الرقمية المثبت على هاتفه المحمول (مستوى المستخدم). تتضمن هذه الخطوة التعرف على المستخدم، والمصادقة، والتفويض، وجمع مدخلات المستخدم (مثل اختيار البطاقة الائتمانية التي سيتم استخدامها)، والبدء في طلب معلومات الدفع مثل المبلغ الذي سيتم دفعه. غالبًا ما تُستخدم البيانات الحيوية لتحديد هوية المستخدم والتحقق منها في هذا المستوى.

02

معالجة عملية الدفع في المستوى الأساسي:
يتم معالجة طلب الدفع من خلال المحفظة الرقمية في المستوى الأساسي. يتم التحقق من صحة المعاملة في مستوى خدمات التطبيقات، وعند مستوى إدارة البيانات يتم استعادة بيانات المستخدم والتحقق منها، بينما تضمن مستوى الأمان والامتثال أن المعاملة تتوافق مع المتطلبات التنظيمية. ويعمل مستوى التكامل والبرمجيات الوسيطة على تمكين التواصل بين المكونات المختلفة، مما يضمن معالجة المعاملة بكفاءة وأمان.

03

إتمام عملية الدفع في المستوى الخارجي:
تقوم المحفظة الرقمية بالاتصال ببوابة الدفع، التي بدورها تتواصل مع بنكي العميل والتاجر لبدء عملية الدفع.

يتم استخدام واجهات برمجة التطبيقات (APIs) اللازمة للتواصل مع البنوك والعلامات التجارية للدفع والتحقق من توفر الأموال لإتمام الدفع، وللحصول على جميع التفويضات اللازمة للمعاملة. ويجب على النظام الأساسي إرسال طلب الدفع بشكل آمن إلى هذه الجهات، حيث تتم معالجة الطلب وتأكيده. وأي إشكاليات قد تحدث في هذه المرحلة النهائية قد تؤدي إلى فشل المعاملات أو حدوث اختراقات أمنية.

ثم يتم جمع تفاصيل المعاملة وتحويل الأموال من حساب المستخدم إلى حساب التاجر. يلي ذلك تحديث تفاصيل المعاملة في المحفظة الرقمية، وإصدار إيصال الدفع للمستخدم.

الشكل 1.3: تحليل عملية الدفع عبر المحفظة الرقمية ضمن سياق البنية الأساسية للتقنية المالية.

بدء الإطلاق والدفع
1. يقوم المستخدم بفتح المحفظة الرقمية واختيار طريقة الدفع (مثل البطاقة الائتمانية أو الحساب البنكي).
2. يتم التحقق من هوية المستخدم.
3. يختار المستخدم التاجر أو يدخل تفاصيل الدفع.
4. يقوم المستخدم ببدء الدفع من خلال تأكيد المبلغ وطريقة الدفع.

إتمام الدفع
1. تستلم المحفظة الرقمية حالة المعاملة.
2. يتلقى المستخدم تأكيد الدفع.
3. يتم تحويل الأموال من حساب المستخدم إلى التاجر.
4. يتم تحديث تفاصيل المعاملة في المحفظة الرقمية.
5. يتلقى المستخدم إيصالًا أو إشعارًا بإتمام المعاملة.

التفاعل عبر بوابة الدفع
1. تتواصل المحفظة الرقمية مع بوابة الدفع.
2. ترسل بوابة الدفع الطلب إلى بنك شبكة الدفع.
3. يقوم البنك أو شبكة الدفع بالتحقق من تفاصيل المعاملة.
4. يتم تفويض المعاملة أو رفضها بناءً على التحقق.

تأسيس ثلاثية تحصين التقنية المالية

تلخيص النقاط الرئيسية في الأمن السيبراني للبنية الأساسية للتقنية المالية

يكشف التحليل الشامل لمسار العملية عن ثلاثة محاور رئيسية تعد أساسية لإتمامها بشكل آمن، والتي تتمثل في واحدة من كل مستوى من البنية الأساسية للتقنية المالية. يمكن أن يؤدي النجاح في اختراق أي من هذه المحاور إلى عواقب كبيرة قد تهدد بقاء البنية الأساسية للتقنية المالية. وتشكل هذه المحاور، التي تحمل اسم "ثلاثية تحصين التقنية المالية"، مخططًا دفاعيًا سيبرانيًا ذا أولوية لمجالس إدارة التقنية المالية، وهي كالآتي:

1. حارس البوابة
2. الوسيط
3. أمين الصندوق

من الضروري أن يستمر أعضاء مجلس الإدارة في مراجعة ثلاثية تحصين التقنية المالية بشكل مستدام للحفاظ على ثقة المستخدم والمجتمع والجهات التنظيمية في حلول التقنية المالية.

الشكل 1.4: ثلاثية تحصين التقنية المالية التي تتطلب إشرافًا مستمرًا على مستوى مجلس الإدارة لضمان الدفاع السيبراني المستمر.

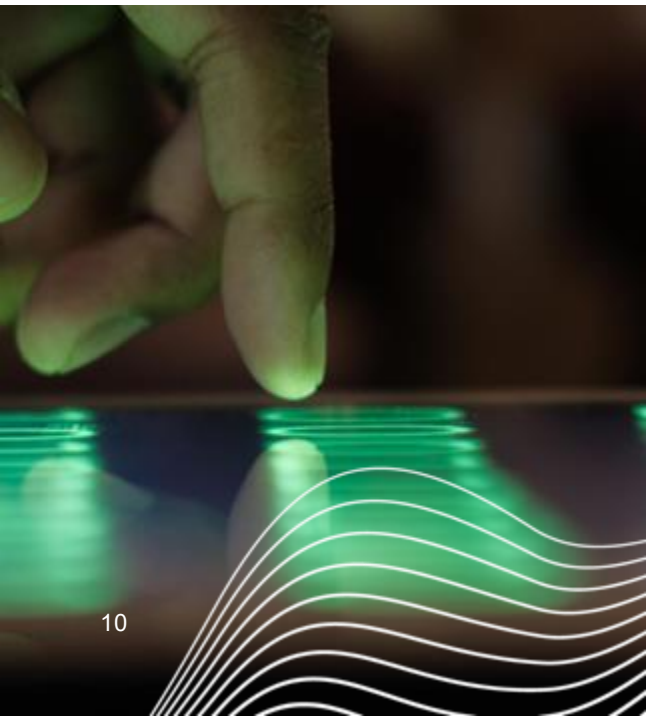
1	**حارس البوابة** إدارة الهوية والوصول	2	**الوسيط** واجهات برمجة التطبيقات APIs))	3	**أمين الصندوق** تكامل بوابة الدفع

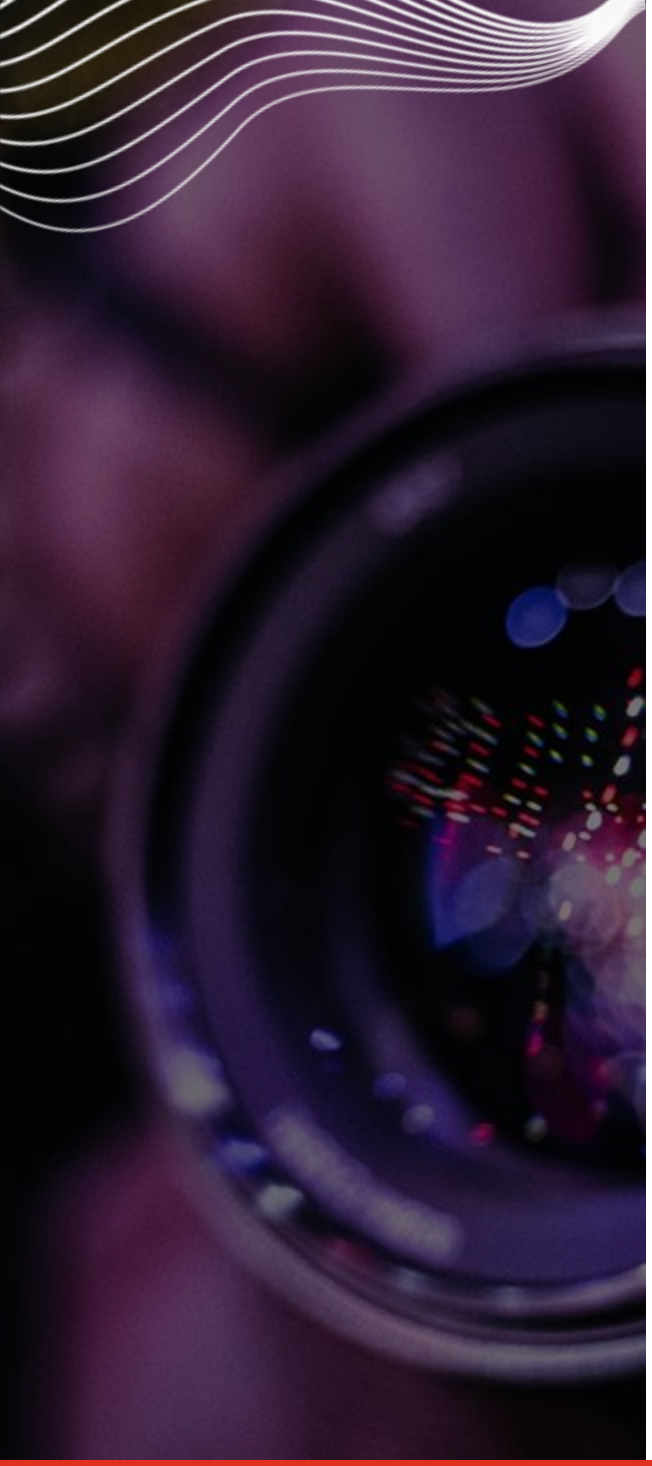
إعداد مخطط على مستوى مجلس الإدارة لإعطاء الأولوية الدفاع السيبراني

01

حارس البوابة (مستوى المستخدم) –
إدارة الهوية والوصول

الخطوة الأولى وهي الخطوة الأكثر أهمية لتأمين معالجة الدفع وهي التحقق من هوية المستخدم. حيث تعمل إدارة الهوية كخط الدفاع الأساسي ضد الوصول غير المصرح به والانتحال. كما تعد نزاهة إدارة الهوية ضرورية لعمل التقنية المالية بشكل آمن. حيث أنه قد يؤدي اختراق الهوية إلى تمكين الجهات الضارة من انتحال شخصية المستخدمين الموثوقين، مما يؤدي إلى معاملات غير مصرح بها، وفقدان البيانات الشخصية، وفرض عقوبات مالية كبيرة. كما تشمل إدارة الهوية آليات مثل التحقق من الهوية متعدد العناصر (MFA)، والتحقق البيومتري (Biometrics)، ومعايير كلمات المرور الآمنة.





02

الوسيط (المستوى الأساسية) –
واجهات برمجة التطبيقات (APIs)

تعد واجهات برمجة التطبيقات (APIs) أدوات لتسهيل التواصل بين مكونات نظام التقنية المالية، سواء داخل النظام الأساسي أو مع الجهات الخارجية. تتيح هذه الواجهات تبادل البيانات بفعالية بين واجهة المستخدم، وأنظمة المعالجة الأساسية، والخدمات الخارجية مثل البنوك أو بوابات الدفع. وفي حال تم اختراقها، يمكن أن تكون واجهة برمجة التطبيقات نقطة دخول للمهاجمين للوصول إلى الأنظمة الحساسة، وسرقة البيانات، أو تعطيل الخدمات.

ولذلك تعد واجهات برمجة التطبيقات جزءًا أساسيًا من عمل التقنية المالية، مما يجعلها مكونًا رئيسيًا يجب مراقبته ضمن مخطط مجلس الإدارة للأمن السيبراني .

03

أمين الصندوق (المستوى الخارجية) –
تكامل بوابة الدفع

تعتبر بوابات الدفع هي الخطوة الأخيرة في العملية، حيث يتم التحويل الفعلي للأموال. تتواصل هذه البوابات مع البنوك، ومعالجي بطاقات الائتمان، والعلامات التجارية للدفع، وغيرها من مقدمي الخدمات المالية لتنفيذ العمليات. يمكن أن تؤدي الثغرات في بوابات الدفع، إذا تم استغلالها، إلى عواقب خطيرة مثل العمليات الاحتيالية، والخسائر المالية، وتضرر سمعة شركات التقنية المالية.

ما الخطوة التالية؟

هذه المقالة هي المقالة الأولى في سلسلة من أربع مقالات من بي دبليو سي الشرق الأوسط، وتسلط الضوء على الحاجة إلى دعم إدارات التقنية المالية في مؤشرات الأداء الرئيسية للأمن السيبراني من منظور تقني مبني على أولويات واضحة. وقد أشارت المقالة إلى ثلاثة محاور أساسية للأمن السيبراني والتي هى حارس البوابة، والوسيط، وأمين الصندوق، والتي يجب على مدراء التقنية المالية الإشراف عليها لتعزيز الثقة والحد من المخاطر السيبرانية. وأكدت المقالة على ضرورة تضمين هذه المحاور الأساسية في أي تقرير على مستوى مجلس الإدارة حول الأمن السيبراني للتقنية المالية.

وستركز مقالاتنا القادمة في هذه السلسلة على كل محور من المحاور الأساسية، كما سيتم توضيح دورها في تحصين الحلول التقنية المالية.

المؤلف:

برافين جوزيف فاكابيل
مدير أول، الاستشارات التقنية،
بي دبليو سي، الشرق الأوسط

المشاركين:

فادي شلهوب
شريك الأمن السيبراني والثقة الرقمية،
بي دبليو سي، الشرق الأوسط

سامر عمر
رئيس الأمن السيبراني والثقة الرقمية،
بي دبليو سي، الشرق الأوسط

عبدالرحمن النجار
استشاري الأمن السيبراني والثقة الرقمية،
بي دبليو سي، الشرق الأوسط

نبذة عن بي دبليو سي

في بي دبليو سي، نساعد عملاءنا على بناء الثقة ومواكبة التغيّر، ليتمكّنوا من تحويل التحديات إلى فرص تنافسية. نحن شبكة عالمية تعتمد على التقنيات الحديثة وكوادرها المتميزة، وتضم أكثر من 370,000 شخص في 149 دولة. من خلال خدماتنا في مجالات التدقيق، والضرائب والقانون، والصفقات، والاستشارات، نساعد على بناء الزخم وتحقيق نتائج مستدامة. لمعرفة المزيد، يُرجى زيارة www.pwc.com.
تضم بي دبليو سي الشرق الأوسط 30 مكتبًا في 12 دولة في المنطقة، ويعمل بها 11,000 شخص، وتجمع بين رؤى إقليمية معمقة وخبرة عالمية لمساعدة العملاء على حل المشكلات المعقدة، ودفع عجلة التحول، وتحقيق نتائج مستدامة. للمزيد من المعلومات، يُرجى زيارة www.pwc.com/me.
بي دبليو سي تشير إلى شبكة بي دبليو سي و/ أو واحدة أو أكثر من الشركات الأعضاء فيها، كل واحدة منها هي كيان قانوني مستقل. للمزيد من المعلومات يرجى زيارة موقعنا www.pwc.com/structure.