درع أوراكل (Oracle Shield)

الدليل الشامل لتأمين قواعد بيانات أوراكل

The Comprehensive Database Security Guide

إعداد: أحمد عبد الفتاح

2026 ©أحمد عبد الفتاح. جميع الحقوق محفوظة.

لا يجوز نسخ، أو إعادة إنتاج، أو توزيع، أو نقل أي جزء من هذا الدليل بأي شكل أو بأي وسيلة—بما في ذلك التصوير، أو التسجيل، أو غيرها من الطرق الإلكترونية أو الميكانيكية—دون الحصول على إذن كتابي مسبق من المؤلف، باستثناء الاقتباسات القصيرة المضمنة في المراجعات النقدية.

إخلاء مسؤولية:

المعلومات والأكواد (Scripts) الواردة في هذا الدليل مقدمة "كما هي" لأغراض تعليمية وإرشادية. على الرغم من بذل أقصى جهد لضمان دقة المحتوى، إلا أن المؤلف لا يتحمل أي مسؤولية قانونية عن أي أضرار مباشرة أو غير مباشرة قد تنشأ عن استخدام الأكواد في بيئات الإنتاج(Production)

يُنصح بشدة باختبار كافة الإعدادات في بيئة اختبار معزولة (Test Environment) قبل تطبيقها.

الإصدار رقم: ١,٠

التاريخ: مايو - ٢٠٢٦

للتواصل والاستشارات **me@ahmedfattah.com**

الموقع الرسمي **https://security.ahmedfattah.com**

Ahmed AbdelFattah

المحتويات

Ahmed AbdelFattah

Ahmed AbdelFattah

Ahmed AbdelFattah

Ahmed AbdelFatah

نبذة عن المؤلف

أحمد عبد الفتاح هو خبير تكنولوجيا أوراكل (Oracle Technology Expert) وحاصل على لقب Oracle ACE ، ويتمتع بخبرة تقنية واسعة تمتد لأكثر من ٣٠ عاماً في مختلف منتجات وخدمات أوراكل. أمضى عشر سنوات في شركة أوراكل، منها خمس سنوات كاستشاري فني أول، وخمس سنوات أخرى كمدير ممارسة الاستشارات التقنية والخبراء في أوراكل لمنطقة مصر وأفريقيا.

على مدار مسيرته المهنية التي غطت منطقة الشرق الأوسط وأفريقيا وأوروبا، قام أحمد بإدارة وقيادة العديد من المشاريع التقنية المعقدة. وتشمل خبرته تنفيذ بيئات السحابة، وترحيل قواعد البيانات إلى منصات Exadata ، وتطبيق حلول التوافر العالي RAC و Data Guard وتحسين الأداء وتصميم وتنفيذ مستودعات البيانات لصالح جهات كبرى في معظم دول المنطقة العربية والأفريقية. كما عمل كمدرب معتمد من أوراكل، حيث قدم دورات تدريبية معتمدة وورش عمل مخصصة للعملاء الرئيسيين في المنطقة.

Ahmed AbdelFatah

مقدمة الدليل الاستراتيجي: حماية السيادة الرقمية في عصر الحروب السيبرانية الهجينة ٢٠٢٦

مشهد التهديدات السيبرانية المعقدة يتطلب رؤية استراتيجية تتجاوز الدفاعات التقليدية.

نحن نعيش اليوم واقعاً رقمياً لم يسبق له مثيل. لقد ولى الزمن الذي كانت فيه حماية قواعد بيانات أوراكل تقتصر على إعدادات جدار الحماية(Firewalls) ، وتطبيق التحديثات الربع سنوية بشكل روتيني، والامتثال الشكلي للمعايير. في ظل التحولات الجيوسياسية المتسارعة التي تشهدها منطقة الشرق الأوسط والعالم، لم تعد الهجمات السيبرانية مجرد احتمالات تقنية أو محاولات فردية لإثبات الذات، بل أصبحت أسلحة استراتيجية تستهدف شريان الحياة للمؤسسات: "البيانات."

تُعد قواعد بيانات أوراكل (Oracle Databases) المستودع الرئيسي لأكثر البيانات حساسية في القطاعات الحيوية، من البنوك والطاقة والدفاع إلى الجهات الحكومية. تشير أحدث الإحصائيات لعام ٢٠٢٦ إلى أن متوسط تكلفة اختراق البيانات قد بلغ ٨,٦٤ مليون دولار أمريكي، مع تعرض مليارات السجلات للسرقة أو التدمير. في هذا السياق، أصبح الاعتماد على الإعدادات الافتراضية (Default Configurations) أو الدفاعات التقليدية بمثابة ترك أبواب الحصن مفتوحة على مصراعيها في ذروة العاصفة.

أولاً: المشهد الإقليمي .. عندما تصبح البيانات ساحة للمعركة

في خضم التصعيد غير المسبوق للتوترات الجيوسياسية، تغيرت قواعد اللعبة بشكل جذري. لم تعد الشبكات أو الأجهزة الطرفية هي الهدف النهائي، بل "البيانات". نحن نعيش اليوم في بيئة ما يُعرف بـ "الاندماج السيبراني الحركي(Cyber-Kinetic Fusion) "، حيث تُشن الهجمات الرقمية بالتوازي مع تصاعد الأحداث الميدانية.

عندما تُصرح الكيانات والمجموعات المعادية المدعومة حكومياً (State-Sponsored Actors) باستهداف البنى التحتية الحساسة، فإنها توجه ضرباتها نحو "القلب النابض" لاقتصادياتنا. قواعد بيانات أوراكل لا تقوم بتشغيل التطبيقات فحسب، بل تحتضن الأسرار المالية، السجلات الحكومية، وبيانات التحكم الصناعي لقطاعات النفط والغاز. إن سقوط قاعدة البيانات يعني شللاً كاملاً للمؤسسة، وتحولاً فورياً من وضع "استمرارية الأعمال" إلى وضع "إدارة الكوارث الوطنية."

اليوم، نشهد تطوراً مرعباً في آليات الهجوم؛ من برمجيات الفدية (Ransomware) التقليدية إلى هجمات المسح التدميرية .(Wiper Malware) هذه المجموعات المنظمة لا تبحث دائماً عن فدية مالية، بل تهدف غالباً إلى محو الوجود الرقمي للمؤسسة بالكامل، مستهدفة تشفير أو حذف ملفات البيانات (Datafiles) والنسخ الاحتياطية بذكاء لقطع أي أمل في خط الرجعة.

ثانياً: فجوة الوثائق الرسمية .. لماذا لا تكفي أدلة أوراكل القياسية؟

أحد الأسئلة الأكثر إلحاحاً التي قد يطرحها القادة التقنيون هو" :لماذا نحتاج إلى هذا الدليل المتخصص بينما توفر شركة أوراكل آلاف الصفحات من الوثائق الرسمية؟"

Ahmed Abdelfattah

القاعدة الذهبية الجديدة لعام ٢٠٢٦ تنص على أن" :الامتثال هو الحد الأدنى، وليس سقف الحماية.(Compliance is the floor, not the ceiling) "

الإجابة تكمن في الفارق الدقيق بين "القاموس النظري" و"خطة النجاة التكتيكية". الوثائق القياسية لأوراكل (Oracle Official Documentation) هي مراجع موسوعية ممتازة، تشرح لك "كيفية" تشغيل التشفير الشفاف (TDE) أو إعداد(Database Vault) ، لكنها تعاني من قيود جوهرية في بيئات العمل الحقيقية المليئة بالتهديدات:

١. **حيادية السياق :(Context Neutrality)** وثائق أوراكل تشرح "كيف" تعمل الخاصية، لكنها لا تخبرك "متى ولماذا" يجب تفعيلها في ظل هجوم سيبراني يستهدف بيئتك التكنولوجية. هي تفترض وجود "مهاجم نظري" أو مستخدم داخلي فضولي، ولا تفرق بين منشأة حيوية تواجه هجمات نوعية من جهات معادية، وبين شركة تجزئة صغيرة.

٢. **التعقيد المفرط وتشتت الانتباه :**لتأمين بيئة أوراكل بالكامل بناءً على الوثائق الرسمية، سيحتاج فريقك إلى قراءة وربط عشرات الأدلة المنفصلة (دليل الأمان، الشبكة، نظام التشغيل). هذا التشتت يخلق ثغرات (Blind Spots) قاتلة عند التطبيق الميداني.

٣. **غياب منظور الأنظمة الهندسية المتكاملة :**غالباً ما تركز الوثائق على قاعدة البيانات ككيان برمجي منعزل، متجاهلة التداخل المعقد في بيئات العمل المتقدمة. تأمين محرك قاعدة البيانات لا قيمة له إذا تم اختراق الشبكة الداخلية (InfiniBand/RoCE) أو عُقد التخزين (Cell Nodes) أو أنظمة/شبكة الإدارة (ILOM) في أنظمة مثل Oracle Exadata

تطبيق مبدأ الثقة المعدومة (Zero Trust) وعزل المهام أصبح ضرورة حتمية لحماية "تاج جواهر" المؤسسات.

هنا تبرز القيمة الحقيقية لهذا الدليل. لقد تم تصميمه ليكون **عصارة خبرة ميدانية طويلة**، حيث تم استخلاص الإجراءات الأكثر حرجاً وتأثيراً، وترجمتها إلى خطوات تنفيذية مباشرة (Actionable Playbooks)لا غنى عنها في وقت الأزمات.

ثالثاً: تشريح التهديدات الخفية وأسلحة ٢٠٢٦ (Threat Intelligence)

Ahmed Abdelfattah

هذا الدليل يختلف جذرياً عن أي مستند تقني آخر، لأنه مبني بالأساس على **استخبارات التهديدات (Threat Intelligence)**. نحن نفترض أن خصمك هو مجموعة منظمة تمتلك موارد هائلة وتكنولوجيا متقدمة. من خلال تحليل الهجمات الأخيرة، يعالج الدليل التكتيكات التالية التي لا تغطيها الوثائق القياسية بشكل كافٍ:

- **فهم تكتيكات ما قبل التشفير (Memory Scraping):** الوثائق تخبرك بتشفير البيانات لحمايتها على الأقراص. لكنها لا تخبرك أن مجموعات التهديد المتقدمة طورت برمجيات خبيثة بلغات حديثة (Rust) و—(Deno) مثل "RustyWater" و—"Dindoor" تُحقن في الذاكرة الحية لسرقة البيانات واستخراج كلمات المرور *قبل* أن تصل إلى مرحلة التشفير على القرص الصلب.

- **التصدي لتسليح الهوية (Identity Weaponization):** المهاجمون اليوم لا يخترقون قواعد البيانات بالقوة الغاشمة، بل "يسجلون الدخول" كمديرين شرعيين. سنوضح كيف تم التخلي عن محاولات كسر التشفير لصالح استغلال ثغرات يوم الصفر في أنظمة إدارة الهوية) مثل الثغرة الحرجة CVE-2026-21992 في(Fusion Middleware) ، وكيف يتم استخدام الذكاء الاصطناعي لشن هجمات قصف الإشعارات (MFA Push Bombing) لإرهاق المستخدمين نفسياً واختراق "العقل البشري."

- **اختراق سلاسل التوريد والتطبيقات الكبرى (Supply Chain):** لا توجد قاعدة بيانات تعمل في فراغ. أصبحت عصابات الابتزاز تستهدف طبقة التطبيقات الكبرى. سنستعرض كيف تم استغلال ثغرات (CVE-2025-61882) في نظام (Oracle E-Business Suite) للكمون لأسابيع واستخراج تيرابايتات من البيانات الحساسة. الأسوأ من ذلك، هو استهداف أجهزة النسخ الاحتياطي) مثل ZDLRA عبر ثغرة (CVE-2026-21977 لضرب سلاسل النسخ الاحتياطي ومنع المؤسسات من التعافي.

رابعاً: ما الذي يجعل هذا الدليل مختلفاً؟

هذا الدليل ليس سرداً نظرياً، بل هو منهجية أمنية متكاملة بُنيت على مبدأ "الدفاع في العمق" (Defense in Depth)وهندسة "انعدام الثقة .(Zero Trust Architecture) "يبرز تفرده وقوته في المحاور التالية:

Ahmed AbdelFattah

- **النهج الشامل للأنظمة المعقدة :(Full-Stack Security)** نحن لا نكتفي بتأمين محرك قاعدة البيانات، بل نوفر خارطة طريق صارمة لتأمين البنية التحتية بالكامل. الدليل يوفر تركيزاً حصرياً ونادراً على تأمين الأنظمة الهندسية(Engineered Systems) ، عبر استراتيجيات مجربة لتأمين خوادم التخزين، إغلاق ثغرات الدعم(ILOM) ، وعزل شبكات الربط العالي السرعة.

- **الامتثال الاستباقي للتشريعات الإقليمية :(Proactive Compliance)** تمت صياغة التوصيات لتتوافق بشكل مباشر مع متطلبات الهيئات الوطنية للأمن السيبراني في الشرق الأوسط، بالإضافة لمعايير (CIS) المحدثة وتوجيهات .(DORA) هذا يوفر على فرق الأمن مئات الساعات من عمليات تعيين المتطلبات (Mapping) على التكوينات التقنية.

- **حماية مسار الترحيل والتحديث :(Secure Migrations)** أخطر فترات الضعف الأمني هي أوقات الترحيل والتحديث. يفرد هذا الدليل مساحة خاصة لضمان عدم تسرب البيانات أو انكشافها أثناء عمليات النقل المعقدة.

- **تجسير الفجوة اللغوية والتقنية :(Bridging the Gap)** بتقديمه باللغة العربية مع الحفاظ على المصطلحات التقنية القياسية، يكسر هذا الدليل الحاجز بين الإدارة العليا التي تتحدث بلغة المخاطر والعوائد(ROI) ، وبين الفرق الفنية (DBAs & System Admins) التي تحتاج إلى أوامر التنفيذ المباشرة.

خامساً: رسالة إلى قادة التكنولوجيا وحراس البيانات

إلى القيادات الأمنية والتنفيذية:(CIOs, CISOs)

إن الاستثمار بملايين الدولارات في رخص أوراكل المتقدمة هو استثمار في الأداء والاعتمادية، لكنه يفقد قيمته تماماً إذا تحولت هذه الأنظمة إلى نقطة الضعف التي تُسقط المؤسسة وتُكبدها خسائر فادحة تتجاوز ملايين الدولارات، بالإضافة للتبعات القانونية ومخاطر غرامات الامتثال المرتبطة باختراقات البيانات. هذا الدليل هو "وثيقة التأمين الاستراتيجية" الخاصة بكم. يوفر لكم إطار عمل واضح لتحويل المحادثات التقنية المبهمة إلى قرارات مبنية على إدارة المخاطر، ويمنحكم القدرة على قياس الأداء الأمني لفرقكم بشكل ملموس وقابل للتدقيق.

Ahmed AbdelFattah

إلى مدراء قواعد البيانات والمهندسين:(Senior DBAs & Cloud Architects)

أنتم خط الدفاع الأخير. في لحظة الهجوم الحقيقي، وفي خضم "الساعة الذهبية" (أول ٦٠ دقيقة من الاختراق)، لن يسعفكم البحث العشوائي في المنتديات أو قراءة آلاف الصفحات النظرية. أنتم بحاجة إلى أداة تكتيكية؛ دليل عملي يضع بين أيديكم الإعدادات الصحيحة، وقوائم المراجعة(Checklists) ، ونصوص التقوية (Hardening Scripts) الحاسمة والمُختبرة .

"الأمان ليس منتجاً تشتريه وتنساه، بل هو عملية مستمرة ويقظة لا تنام. وفي عالم أوراكل، التفاصيل الدقيقة هي التي تصنع الفارق بين مؤسسة صامدة، ومؤسسة تتصدر عناوين الأخبار كضحية جديدة".

هذا الدليل صُنع ليحمي بيانات مؤسساتكم، ويحمي مسيرتكم المهنية في أحلك اللحظات.

دعونا نبدأ رحلة تحصين أصولكم الرقمية الأغلى.

Ahmed Atef Eatah

الفصل الأول: المشهد الاستراتيجي: الجيوسياسة تلتقي بأمن البيانات(2026)

إن فهم التهديد هو نصف المعركة. تُعد قواعد بيانات أوراكل (Oracle Databases) والأنظمة الوسيطة المرتبطة بها بمثابة العصب الحيوي للبنى التحتية المعلوماتية، حيث تعتمد عليها قطاعات الطاقة، والتمويل، والخدمات الحكومية، والدفاع بشكل شبه كامل لإدارة البيانات الحساسة وعمليات صنع القرار. ومع التصعيد العسكري غير المسبوق الذي اجتاح مناطق التوتر الإقليمي مطلع عام ٢٠٢٦، تحول الفضاء السيبراني إلى ساحة معركة موازية لا تقل ضراوة عن العمليات الميدانية. في هذا الفصل، نُحلل كيف انعكست التوترات الجيوسياسية على أمن البنى التحتية التقنية، وكيف تطورت عقيدة المهاجمين من "التجسس" إلى "التدمير."

١,١ الاندماج السيبراني الحركي (Cyber-Kinetic Fusion) كواقع جديد

في الماضي القريب، كانت الهجمات السيبرانية الإقليمية تتركز حول التجسس طويل الأمد، أو عمليات التخريب المعزولة، أو التشهير (Hacktivism) أما اليوم، فقد ظهر مصطلح "**الاندماج السيبراني الحركي**". يعني هذا المفهوم أن الهجمات الرقمية تُشن بطريقة متزامنة ومدروسة لدعم أهداف عسكرية وجيوسياسية على الأرض.

في أواخر فبراير ومطلع مارس ٢٠٢٦، وتحديداً مع انطلاق العمليات العسكرية الميدانية واسعة النطاق، شهدنا اندماجاً كاملاً بين العمليات الحركية والسيبرانية. أدت الهجمات المكثفة والمتبادلة إلى انقطاع شبه كامل للإنترنت في بعض المناطق المستهدفة، حيث انخفضت نسبة الاتصال إلى ٤٪ فقط من مستوياتها الطبيعية. في المقابل، واجهت المؤسسات الحيوية في المنطقة موجة انتقامية هائلة غير مسبوقة في حجمها وسرعتها.

نحن نتحدث اليوم عما يُعرف بـ "**مشكلة الـ ٠,٠١%**"؛ فحينما يشن الخصم ١,٥ مليون هجوم سيبراني في غضون ٧٢ ساعة، فإن حتى الدفاعات التي تعمل بكفاءة ٩٩,٩٩٪ ستسمح بمرور اختراقات قادرة على تدمير أنظمة بأكملها.

التغير الأخطر بالنسبة لمديري قواعد البيانات (DBAs) هو التحول نحو **البرمجيات التدميرية والماسحة (Wipers)** لم يعد الهدف هو احتجاز البيانات لطلب فدية، بل تدميرها. استخدمت

مجموعات التهديد المتقدمة (APTs) الإقليمية طفرات برمجية ماسحة مثل Shamoon ، Agonizing Serpens، Tickler ، و SHAPESHIFT هذه البرمجيات تستهدف تدمير قطاعات التشغيل الرئيسية (MBR) وملفات قواعد البيانات بشكل لا رجعة فيه لإحداث شلل تشغيلي حاسم، خاصة في قطاعات الطاقة (OT/ICS) والرعاية الصحية والمطارات. في هذا السيناريو، إذا تم اختراق قاعدة بيانات أوراكل، فإن الهدف النهائي هو محوها بالكامل، مما يجعل الاعتماد المفرط على النسخ الاحتياطية المتصلة بالشبكة خطراً قاتلاً.

١,٢ تطورترسانة التهديد: الذكاء الاصطناعي واللغات الآمنة

لفهم كيفية حماية قواعد بيانات أوراكل، يجب أن نفهم أولاً الأدوات التي يستخدمها المهاجمون. لقد تخلت المجموعات المتقدمة عن أدواتها التقليدية ونفذت حملات استراتيجية واسعة) مثل عملية ."Operation Olalampo") لقد تطورت تكتيكات هذه المجموعات بشكل جذري وغير مسبوق لتجاوز الجيل الحديث من مضادات الفيروسات:

الذكاء الاصطناعي التوليدي :(Offensive GenAI) بدلاً من قضاء أسابيع في البرمجة وتطوير أدوات مخصصة، تستخدم هذه المجموعات اليوم نماذج اللغات الكبيرة (LLMs) لشن هجمات دقيقة. يتم توليد نصوص تصيد احتيالي (Phishing) خالية من العيوب مصممة خصيصاً لاستهداف مديري قواعد البيانات، وكتابة أكواد خبيثة متغيرة (Polymorphic) لحظياً لتجاوز أنظمة الكشف(Just-in-Time Malware)

الانتقال إلى لغات Rust و Deno لتجنب اكتشافها من قبل أنظمة الكشف والاستجابة على نقاط النهاية (EDR) ، طورت المجموعات برمجيات اختراق متقدمة (Implants) مثل RustyWater المكتوبة بلغة Rust وبرمجية Dindoor المبنية على بيئة Deno الميزة الأخطر لهذه البرمجيات هي قدرتها على العمل بالكامل داخل الذاكرة الحية (Memory Scraping) وسرقة البيانات قبل وصولها لمرحلة التشفير، متجنبة ترك أي آثار (Fileless) قابلة للكشف على القرص الصلب.

البوابات الخلفية المتعددة المراحل :(Multi-stage Backdoors) تم رصد استخدام برمجيات معقدة مثل Fakeset و Stagecomp التي تقوم لاحقاً بتحميل برمجيات Darkcomp للكمون داخل شبكات المطارات والمنظمات غير الربحية والبنوك لفترات طويلة.

Ahmed Abdelfatah

التخفي عبر قنوات مشروعة (C2 Evasion): لتهريب البيانات المسروقة من قواعد البيانات (Data Exfiltration)، تقوم المجموعات بتوجيه حركة المرور الخبيثة عبر خوادم وبروتوكولات مشروعة؛ مثل استخدام واجهة برمجة تطبيقات تيليجرام (Telegram Bot API) أو الاعتماد على قنوات DNS Tunneling المعقدة، مما يجعل حركة البيانات تبدو اعتيادية جداً ويصعب على الجدران النارية (Firewalls) حظرها دون تعطيل العمل.

إلى جانب ذلك، برز دور العمليات النفسية وحرب المعلومات؛ حيث قامت المجموعات التخريبية (Hacktivists) باختراق بوابات بث (IPTV) ومنصات إعلامية لثني الرأي العام، واستخراج تيرابايتات من العقود الحساسة والسجلات المالية لشركات طاقة إقليمية رائدة بغرض التشهير والابتزاز (Doxxing)

١,٣ استراتيجية تسليح الهوية Identity Weaponization اختراق الحراس بدلاً من الأسوار

أكبر خطأ استراتيجي يقع فيه مديرو أمن المعلومات (CISOs) اليوم هو تركيز الميزانية بالكامل على تأمين قاعدة البيانات من الداخل من خلال التشفير، بينما يُترك "الباب الأمامي" للهوية مشرعاً.

في مارس ٢٠٢٥، صُدم المجتمع التقني بإعلان مخترق يُدعى (rose87168) عن اختراق خوادم تسجيل الدخول الخاصة بسحابة أوراكل(Oracle Cloud) ، مما أتاح الوصول إلى أنظمة الدخول الموحد (SSO) لعدد ضخم تجاوز ١٤٠ ألف مستأجر (Tenant) هذا الحدث يجسد التكتيك الحديث والأخطر :**تسليح الهوية**.

المهاجم المتقدم اليوم لا يضيع وقته في محاولة كسر التشفير الشفاف لبيانات أوراكل (TDE) باستخدام القوة الغاشمة، بل يستولي على هويات الإدارة الشرعية. بمجرد أن يسجل المهاجم دخوله بصفته مدير النظام(DBA) ، تصبح كافة أدوات التشفير بلا جدوى، لأن قاعدة البيانات تقوم تلقائياً بفك تشفير البيانات لتقديمها للمستخدم الذي تعتقد أنه يمتلك الصلاحية. يتم تحقيق ذلك من خلال:

قصف الإشعارات (MFA Push Bombing / MFA Fatigue): استخدام خوارزميات الذكاء الاصطناعي لإغراق هواتف مديري قواعد البيانات بطلبات مصادقة مستمرة في أوقات متأخرة

Ahmed Abdelfattah

من الليل، لدفعهم نفسياً—بدافع الإرهاق—للموافقة عليها، مما يمنح المهاجم وصولاً إدارياً كاملاً.

استغلال ثغرات أنظمة الهوية :تتجلى خطورة هذا التكتيك في الاستغلال السريع للثغرات الحرجة، مثل ثغرة (CVE-2026-21992) المكتشفة في أنظمة إدارة الهوية المرتبطة بأوراكل (Oracle Identity Manager)و (Web Services Manager) تتيح هذه الثغرة للمهاجمين تنفيذ أوامر برمجية عن بُعد (RCE) دون مصادقة، مما يمكنهم من السيطرة الكاملة على نظام إدارة الهوية المركزي.

١,٤ استهداف سلاسل التوريد وموقع التعافي كخيار استراتيجي

في سياق الحروب الهجينة لعام ٢٠٢٦، يدرك المهاجمون أن تدمير قاعدة البيانات سيكون بلا تأثير حقيقي إذا استطاعت المؤسسة استعادتها من النسخ الاحتياطية في غضون ساعات. لذا، تحولت عقيدة المهاجمين نحو" **تدمير القدرة على التعافي** "واختراق" **سلاسل التوريد البرمجية**."

اختراق التطبيقات المؤسسية الكبرى :استهدفت مجموعات التهديد المتقدمة أنظمة ضخمة مبنية على قواعد بيانات أوراكل، مثل (Oracle E-Business Suite) عبر استغلال ثغرات صفرية (CVE-2025-61882) من خلال حقن قوالب خبيثة(Malicious Templates) ، تمكن المهاجمون من الكمون لأسابيع واستخراج كميات مهولة من السجلات المالية وسجلات المشتريات، متجاوزين بذلك طبقات أمان محرك قاعدة البيانات الأساسي.

تدمير النسخ الاحتياطية :(Backup Annihilation) تم رصد استهداف مباشر لأجهزة التعافي الحساسة، مثل أجهزة (Oracle Zero Data Loss Recovery Appliance - ZDLRA) عبر ثغرات مثل (CVE-2026-21977) يهدف المهاجمون من خلال ذلك إلى الوصول لبيانات النسخ الاحتياطي، وحذفها، أو تشفير مفاتيحها، لضمان أن الهجوم التدميري اللاحق (Wiper) سيقضي على المؤسسة بشكل نهائي.

Ahmed AbdelFattah

١,٥ الخلاصة الاستراتيجية للقيادة (Executive Takeaway)

إن الجغرافيا السياسية لعام ٢٠٢٦ قد حولت "بيانات المؤسسات" إلى بنية تحتية حرجة توازي في أهميتها محطات الطاقة أو منشآت تحلية المياه. بالنسبة لقادة أمن المعلومات(CISOs) ، لم يعد مبرراً النظر إلى تأمين قواعد بيانات أوراكل كمسألة صيانة تقنية بحتة تندرج تحت الميزانيات الروتينية لإدارة تكنولوجيا المعلومات (IT)

يجب رفع مستوى النقاش فوراً إلى مجالس الإدارة:(Board of Directors)

الامتثال ليس كافياً :إن الفشل في تأمين قواعد البيانات ومحيطها لا يعني فقط التعرض لغرامات لعدم الامتثال، بل يعني تعرض المؤسسة لشلل تشغيلي ووجودي كامل لا رجعة فيه.

النسخ الاحتياطية المعزولة :(Air-gapped) يجب ضمان وجود نسخ احتياطية غير قابلة للتعديل أو الوصول عبر الشبكة العادية (Offline Backups)

تطبيق الثقة المعدومة :(Zero Trust) يجب التخلي عن عقلية "أن شبكتنا الداخلية آمنة"، والتحول الفوري نحو تقييد صلاحيات مديري الأنظمة أنفسهم عبر تقنيات مثل Oracle) (Database Vault، وربطها بالتحليل الاستباقي للتهديدات.

هذا التحول الجذري في التفكير الأمني هو الأساس الذي تُبنى عليه الفصول التقنية القادمة في هذا الدليل.

Ahmed Abdelfatah

الفصل الثاني: تقييم وإدارة المخاطر في بيئة أوراكل (الثغرات، الأدوات، وسلاسل التوريد)

لا يمكنك حماية ما لا تفهمه؛ التقييم المستمر للمخاطر هو الخطوة الأولى نحو السيادة الرقمية.

لم تعد إدارة الثغرات (Vulnerability Management) في عام ٢٠٢٦ مجرد مهمة روتينية لفرق تكنولوجيا المعلومات للامتثال للمعايير؛ بل أصبحت سباقاً مع الزمن ضد مجموعات التهديد المتقدمة (APTs) التي باتت تستغل الثغرات المكتشفة حديثاً خلال ٢٤ إلى ٤٨ ساعة فقط.

في هذا الفصل، ننتقل من التنظير إلى التشريح التقني لكيفية استهداف قواعد بيانات أوراكل وتطبيقاتها، وكيفية استخدام أدوات أوراكل الأصلية لسبق المهاجمين بخطوة.

٢,١ الثغرات الصفرية والحرجة: أمثلة تشريحية من أرض الواقع

تستهدف مجموعات التهديد المتقدمة طبقات متعددة للوصول إلى بيانات أوراكل. إليك أبرز الثغرات المستغلة حالياً وكيفية عملها:

أولاً: اختراق أنظمة الهوية (CVE-2026-21992)

طبيعة التهديد :ثغرة حرجة (بدرجة خطورة ٩,٨) تضرب أنظمة (Oracle Identity Manager) و(Oracle Web Services Manager).

سيناريو الهجوم :لا يحاول المهاجم هنا كسر تشفير قاعدة البيانات المعقد، بل يستهدف "حارس البوابة". تتيح هذه الثغرة للمهاجم تنفيذ أوامر برمجية عن بُعد (RCE) عبر الشبكة دون الحاجة لأي مصادقة أو اسم مستخدم. بمجرد السيطرة على نظام الهوية، يقوم المهاجم بمنح نفسه صلاحيات (DBA) مشروعة، مما يجعل جميع أدوات التشفير (TDE) عديمة الفائدة، لأن النظام سيفك التشفير تلقائياً لـ "المدير الشرعي."

ثانياً: التسلل عبر تطبيقات المؤسسات الكبرى حملة CL0P و Oracle EBS

طبيعة التهديد :استغلال ثغرات يوم الصفر) مثل CVE-2025-61882 و-CVE-2025-61884)في نظام.(Oracle E-Business Suite - EBS)

سيناريو الهجوم (كيف تمت السرقة) :في أغسطس ٢٠٢٥، بدأ المهاجمون بتوجيه طلبات خبيثة إلى مكون يُدعى `SyncServlet` داخل خوادم EBS باستخدام ميزة إدارة القوالب (XDO Template Manager)، قاموا بحقن قوالب خبيثة، ثم فعلوها عبر ميزة "معاينة القالب". النتيجة؟ تمكن المهاجمون من تشغيل أوامر استطلاع خطيرة تحت صلاحيات حساب التطبيق) `applmgr` مثل `cat /etc/fstab` وفتح اتصال عكسي عبر (`/bin/bash -i` مكث المهاجمون أسابيع داخل النظام واستخرجوا تيرابايتات من البيانات المالية والمشتريات دون المساس المباشر بمحرك قاعدة البيانات الأساسي.

إجراء استباقي وفوري:(Hunting Script)

للتحقق من سلامة بيئة (EBS) من هذا النوع من الهجمات، يجب على فرق الاستجابة للحوادث تشغيل استعلامات دورية للبحث عن القوالب المشبوهة التي يبدأ اسمها بـ `TMP` أو`DEF` ، والتي تُمثل مؤشراً قوياً على الاختراق:

```
-- صيد القوالب الخبيثة المحتملة في بيئة Oracle EBS حملات CL0P

--تحذير: تجنب استخدام الأسماء المستعارة المحظورة وتمسك بالأسماء القياسية.
```


Ahmed AbdelFattah

```
SELECT
    t.template_code,
    t.creation_date,
    l.lob_code
FROM
    xdo_templates_b t
JOIN
    xdo_lobs l ON t.template_code = l.lob_code
WHERE
    t.template_code LIKE 'TMP%'
    OR t.template_code LIKE 'DEF%'
ORDER BY
    t.creation_date DESC;
```

ثالثاً: ضرب خطوط العودة والنسخ الاحتياطي (CVE-2026-21977)

طبيعة التهديد :استهداف جهاز أوراكل المخصص للتعافي من الكوارث (Zero Data Loss Recovery Appliance).

سيناريو الهجوم :في هجمات البرمجيات الماسحة(Wipers) ، يعلم المهاجم أن نسختك الاحتياطية هي طوق نجاتك. يقوم المهاجم باستخدام بروتوكول شبكة أوراكل (Oracle Net) عبر المنفذ ١٥٢١، وبتوظيف تقنيات الهندسة الاجتماعية، يتمكن من استخراج وقراءة بيانات التعريف (Metadata) الخاصة بالنسخ الاحتياطية. هذا الاستطلاع يمهد الطريق لتدمير مسارات التعافي قبل إطلاق الهجوم التدميري.

٢,٢ استخدام أدوات التقييم المتقدمة: كيف تسبق المهاجم؟

لا يمكنك حماية ما لا تفهمه، ولا يمكنك سد ثغرات لا تراها. لحسن الحظ، توفر أوراكل أداتين استراتيجيتين يجب أن تكونا ضمن الترسانة اليومية لأي (DBA) و(CISO):

١. أداة تقييم أمان أوراكل :(DBSAT 4.0) الفحص التكتيكي العميق

أداة مجانية وسريعة، تتكون من ثلاثة أجزاء) المُجّمعCollector ، والمُقررReporter ، والمُكتشف .(Discoverer في إصدارها الحديث (٤,٠)، تقدم الأداة ميزات لا غنى عنها:

ربط التحديثات المفقودة بأسماء الثغرات (CVE Mapping): بدلاً من إخبارك بأنك متأخر في التحديثات، سيخبرك تقرير DBSAT 4.0 بشكل صريح: "عدم تطبيق هذا التحديث يتركك عرضة للثغرة"CVE-2026-21929 ، مما يساعد الـ CISO في تسويغ طلبات التوقف (Downtime) الطارئة للإدارة العليا.

تقييم المستخدمين والصلاحيات المفرطة: تكتشف الأداة الحسابات الافتراضية التي تُركت بكلمات مرور قياسية (مثل حساب `SCOTT` أو `HR`) والتي يمتلك المهاجمون نصوصاً برمجية جاهزة لتجربتها. كما تحدد بدقة الحسابات الخاملة التي لم تسجل دخولاً لفترة طويلة (والتي يستخدمها المهاجمون كأبواب خلفية خفية).

اكتشاف البيانات الحساسة (Data Discovery): تبحث الأداة في قواميس البيانات وتخبرك بدقة: "لديك ١٠ ملايين سجل لبطاقات ائتمان غير مشفرة في الجدول X ضمن المخطط Y" ، مما يتيح لك توجيه ميزانية التشفير (TDE) للأماكن الصحيحة.

٢. المراقبة المستمرة باستخدام Oracle Data Safe واكتشاف الانحراف (Drift Detection)

أداة سحابية (متاحة أيضاً للبيئات المحلية)، تتميز بقدرتها على تحويل التقييم من "لقطة لمرة واحدة" إلى "مراقبة مستمرة."

ميزة اكتشاف الانحراف (Security Drift): تقوم بتحديد "خط أساس (Baseline) "آمن لقاعدة البيانات. إذا قام مبرمج في منتصف الليل بمنح صلاحية DBA لحساب تطبيق اختباري لتسهيل عمله، سيطلق Data Safe تنبيهاً فورياً بوجود "انحراف أمني"، مما يمنع تحول هذا الخطأ لثغرة يستغلها المهاجمون.

تنقيح وإخفاء البيانات (Data Masking): استنساخ قواعد بيانات الإنتاج إلى بيئات التطوير (Dev/Test) ينقل المخاطر كاملة. يوفر Data Safe أدوات لإخفاء البيانات الحساسة ببيانات وهمية واقعية، بحيث لو أُخترقت بيئة التطوير، لا تتسرب أي بيانات حقيقية.

Ahmed Abdelfattah

٢,٣ مخاطر سلاسل التوريد والبيئة المحيطة (Supply Chain & Ecosystem Risks)

تدرك مجموعات التهديد المتقدمة أن اختراق جدران الحماية للشركات الكبرى قد يكون مكلفاً. لذلك، ركزت الهجمات الإقليمية مؤخراً بشكل مكثف على سلاسل التوريد وموفري الخدمات ذوي الوصول الموثوق:(Trusted Access)

الاختراق عبر الأطراف الثالثة :(Third-Party Compromise) في حملة ابتزاز (Oracle EBS) الأخيرة، استخدم القراصنة مئات الحسابات المخترقة لشركات خارجية (موردين ومقاولين) لإرسال رسائل الابتزاز إلى المديرين التنفيذيين للشركات المستهدفة، مستغلين الثقة الممنوحة لهذه الحسابات لتجاوز فلاتر البريد المزعج(Spam Filters)

حالة برمجية Fantasy الماسحة :أظهرت مجموعات متقدمة تطوراً مرعباً حين اخترقت شركة تطوير برمجيات إقليمية، واستخدمت تحديثات برامج هذه الشركة (Supply-chain attack) كحصان طروادة لنشر برمجية `Fantasy` الماسحة والمدمرة للبيانات لدى عملاء الشركة المطورة.

توصية استراتيجية :لا يجب أن تثق قاعدة بيانات أوراكل بأي اتصال لمجرد أنه قادم من شبكة مقاول أو عبر شبكة VPN الخاصة بالدعم الفني. يجب تطبيق مبدأ "الثقة المعدومة " (Zero Trust) وفرض المصادقة متعددة العوامل (MFA) وتقييد وصول الموردين إلى "أقل الصلاحيات" المطلوبة وفقط أثناء أوقات الصيانة المجدولة.

٢,٤ الخلاصة التشغيلية للـ CISO والـ DBA

إن إدارة المخاطر في عام ٢٠٢٦ هي سباق مع الزمن.

أتمتة التقييم :يجب تفعيل (Data Safe) أو تشغيل (DBSAT) شهرياً كحد أدنى. التقارير اليدوية السنوية أصبحت من الماضي.

Ahmed Abdelfattah

الترقيع الطارئ (Emergency Patching): الإعلانات الأمنية خارج الدورة المعتادة (Out-of-cycle)، مثل التنبيهات الخاصة بـ EBS وإدارة الهوية، تتطلب تطبيقاً فورياً خلال ساعات (SLA)، وليس أسابيع.

مراقبة السلوك التطبيقي: الهجمات عبر التطبيقات (EBS) تؤكد أن تأمين محرك قاعدة البيانات يجب أن يترافق مع مراقبة نشطة للأوامر القادمة من التطبيقات الصديقة، وهو ما سيقودنا في الفصول القادمة للحديث عن ميزة (SQL Firewall)

Ahmed AbdelFattah

الفصل الثالث: تحصين النواة - الدفاع في العمق لقواعد بيانات أوراكل

لا يمكن بناء درع متطور من أدوات الذكاء الاصطناعي فوق أساسات هشة؛ تحصين النواة هو الخطوة التي لا تقبل المساومة.

في ظل التهديدات المتقدمة التي نشهدها في عام ٢٠٢٦، أثبتت الاستراتيجيات الأمنية التقليدية التي تعتمد حصرياً على تأمين محيط الشبكة (Network Perimeter) فشلها الذريع. فبمجرد نجاح المهاجمين في اختراق الشبكة الداخلية، تصبح قاعدة البيانات هدفاً مكشوفاً.

هذا الفصل يضع خارطة طريق تقنية وتنفيذية لمديري أمن المعلومات (CISOs) ومديري قواعد البيانات (DBAs) لتطبيق بنية أوراكل الأمنية القصوى (Maximum Security Architecture) ، بحيث تتحول قاعدة البيانات نفسها إلى قلعة حصينة قادرة على الدفاع عن نفسها من الداخل حتى لو سقطت دفاعات الشبكة الخارجية، بدءاً من التشفير وعزل المهام، وصولاً إلى تجريد الصلاحيات القاتلة وسد منافذ الاستطلاع.

Ahmed Attar

٣,١ التشفير الشفاف للبيانات (TDE) وحماية البيانات في وضع السكون

الخطوة الدفاعية الأولى والأهم هي إدراك أن اختراق نظام التشغيل (OS) لا ينبغي أن يعني بالضرورة اختراق البيانات. مجموعات التهديد المدعومة حكومياً تستغل غالباً صلاحيات نظام التشغيل لنسخ ملفات قاعدة البيانات (Datafiles) أو ملفات النسخ الاحتياطي ونقلها إلى خوادمها.

سيناريو الهجوم الاستخباري: إذا تمكن مهاجم من الحصول على وصول جذري (Root) لنظام التشغيل، يمكنه ببساطة استخدام أوامر لينكس الأساسية مثل `strings` لقراءة محتوى ملفات قاعدة البيانات ذات الامتداد (`.dbf`) في غياب التشفير، ستظهر كلمات المرور، وأرقام بطاقات الائتمان، والبيانات الصحية كنصوص واضحة (Clear-text) يمكن قراءتها وسرقتها بسهولة شديدة.

التطبيق والتخفيف :(Mitigation) يجب تفعيل التشفير الشفاف للبيانات (TDE) لتشفير مساحات الجداول (Tablespaces) بالكامل. عند تفعيل (TDE) باستخدام خوارزميات التشفير المتقدمة مثل(AES256) ، تتحول البيانات داخل الملفات إلى نصوص مشفرة غير مقروءة(Ciphertext) ، مما يجعل الملفات المسروقة عديمة القيمة تماماً للمهاجم.

إدارة المفاتيح ومقاومة الحوسبة الكمية :(Quantum-Resistance) لا تقم بتخزين مفاتيح التشفير على نفس الخادم الذي يحوي قاعدة البيانات. يُنصح بشدة باستخدام حلول إدارة المفاتيح الخارجية مثل (Oracle Key Vault) علاوة على ذلك، ولمواجهة هجمات "احصد الآن وفك التشفير لاحقاً (Harvest now, decrypt later) " التي تشنها الدول لتخزين البيانات المشفرة بانتظار تطور الحواسيب الكمية، أتاحت أوراكل في تحديثات ٢٠٢٦ إصدار ai ٢٦ استخدام خوارزميات التشفير الهجينة المقاومة للكم مثل(ML-KEM) لتأمين اتصالات الشبكة، مما يضيف طبقة درع مستقبلية لا غنى عنها.

Ahmed Abdelfattah

٣,٢ تفعيل خزنة قاعدة البيانات (Oracle Database Vault) وعزل المهام

التهديد الأكبر لأي قاعدة بيانات هو حساب مدير قاعدة البيانات (DBA) المخترق. المهاجمون يعلمون أن حسابات مثل `SYS` أو `SYSTEM` تمتلك "مفاتيح المملكة"، ولذلك يركزون على سرقة بيانات اعتماد الإدارة عبر التصيد أو اختراق الأجهزة الطرفية(Identity Weaponization)

استخدام النطاقات :(Realms) يقوم نظام (Database Vault) بتطبيق مبدأ "الفصل بين المهام .(Separation of Duties) "من خلال إنشاء "نطاقات(Realms) "، يمكن وضع الجداول الحساسة (مثل جداول الرواتب أو البيانات الطبية) داخل صندوق افتراضي آمن. حتى لو تم اختراق حساب يمتلك صلاحيات الإدارة الكاملة (DBA) أو`SYSDBA` ، فإنه سيُمنع تماماً من عرض البيانات الحساسة أو التعديل عليها ما لم يتم إضافته بشكل صريح ك "مشارك مصرح له (Authorized Participant) "في هذا النطاق المخصص.

قواعد الأوامر (Command Rules) لمقاومة التدمير :يتيح النظام تقييد أوامر محددة داخل قاعدة البيانات، وهو أمر بالغ الأهمية لمواجهة البرمجيات التدميرية (Wipers) التي تستهدف مسح البيانات. على سبيل المثال، يمكن إنشاء قاعدة تمنع تنفيذ أمر `DROP TABLE` أو `TRUNCATE` بشكل قاطع وفي كافة الأوقات، حتى للمستخدمين المصرح لهم ولأصحاب المخططات(Schema Owners) ، مما يُحيد قدرة المهاجمين الداخليين أو الخارجيين على تدمير بنية البيانات.

٣,٣ التطبيق الصارم لمبدأ "أقل الصلاحيات" وتقييد الحزم العامة

إن التكتيك الأبرز للمهاجمين اليوم للتحرك أفقياً (Lateral Movement) داخل النظام يعتمد على استغلال الصلاحيات المفرطة التي تُمنح عادة للمستخدمين والتطبيقات لتسهيل العمل. يجب تطبيق "مبدأ أقل الصلاحيات (Principle of Least Privilege - PoLP) "بصرامة، بحيث لا يمتلك أي مستخدم—أو حتى مطور—صلاحيات تتجاوز ما يحتاجه لإنجاز مهمته الحالية فقط.

أولاً: الخطر الأكبر في المنح المباشر للصلاحيات النظامية

Ahmed AbdelFattah

يقوم العديد من مديري قواعد البيانات (DBAs) بمنح صلاحيات شاملة مثل `DBA` ، أو `SELECT ANY TABLE`، أو `GRANT ANY PRIVILEGE` مباشرة للمستخدمين أو حسابات التطبيقات. في حال سقطت بيانات اعتماد هذا التطبيق في أيدي المهاجم، فإنه يحصل على تحكم كامل بالبيئة.

يجب نقل كافة الصلاحيات لتدار عبر "الأدوار (Roles) " المخصصة بدلاً من المنح المباشر. وفي الإصدارات الحديثة مثل ٢٣ c و ai٢٦، يجب الاستفادة من ميزة **صلاحيات مستوى المخطط (Schema-level privileges)** بدلاً من منح المستخدم حق الوصول إلى جميع جداول قاعدة البيانات، يتيح لك أمر واحد حصر الوصول في المخطط المطلوب فقط (مثال `GRANT SELECT ANY TABLE ON SCHEMA SALES TO SCOTT`)، مما يقلل من مساحة الهجوم بشكل هائل.

استخدم السكربت التالي للكشف الفوري عن الحسابات التي تملك صلاحيات نظامية خطيرة بشكل مباشر (مع استثناء الحسابات النظامية الافتراضية لأوراكل):

```
--صيد الحسابات ذات الصلاحيات النظامية المباشرة والمفرطة
--تحذير: تم الالتزام بعدم استخدام أسماء مستعارة محظورة وتمسك بالقياسية
SELECT
    sp.grantee AS account_name,
    sp.privilege AS dangerous_privilege,
    sp.admin_option
FROM
    dba_sys_privs sp
JOIN
    dba_users u ON sp.grantee = u.username
WHERE
    u.oracle_maintained = 'N'
    AND sp.privilege IN (
        'DBA',
        'GRANT ANY PRIVILEGE',
        'ALTER ANY SYSTEM',
        'SELECT ANY TABLE',
        'DROP ANY TABLE',
        'CREATE ANY PROCEDURE'
    )
ORDER BY
    sp.grantee;
```

ثانياً: تقييد الحزم البرمجية العامة (PUBLIC Grants)

تحتوي قواعد بيانات أوراكل على حزم برمجية قوية مدمجة (مثل UTL_TCP للاتصالات الشبكية، و UTL_FILE لملفات النظام، و DBMS_CRYPTO للتشفير). منح صلاحية التنفيذ (EXECUTE) على هذه الحزم للمجموعة العامة (PUBLIC) يمثل ثغرة كارثية، حيث يمكن لأي مستخدم عادي استغلالها لفتح اتصالات عكسية مع خوادم المهاجمين (C2) أو قراءة ملفات حساسة. يجب فوراً إلغاء هذه الصلاحيات من PUBLIC وحصرها في المستخدمين الذين يحتاجونها للعمل الفعلي فقط.

ثالثاً: تنويه هام للمطورين(DB_DEVELOPER_ROLE)

لتجنب منح المطورين صلاحيات عشوائية، أضافت أوراكل حديثاً دور DB_DEVELOPER_ROLE ورغم أنه أفضل بكثير من منح صلاحية DBA ، إلا أنه يجب التحذير من الاعتماد الحرفي والمطلق عليه في بيئات الإنتاج (Production) ، حيث يتضمن صلاحيات قد تُستغل للاستطلاع من قبل المهاجم المتقدم. يجب أن يقتصر استخدامه حصراً على بيئات التطوير والاختبار (Non-Prod)

٣,٤ إغلاق الثغرات التكوينية (Initialization Parameters Hardening)

تُعد معلمات التهيئة (Initialization Parameters) بمثابة أبواب خلفية إذا لم يتم ضبطها بشكل صحيح، وقد استخدمها المهاجمون مراراً لتنفيذ أوامر على مستوى نظام التشغيل (OS) أو لتجاوز آليات التدقيق وفقاً لتقارير الامتثال لمعايير (CIS Benchmarks)

لتحصين النواة، يجب فحص وتعديل المعلمات التالية عبر: ALTER SYSTEM

منع الوصول غير المصرح به للملفات :(UTL_FILE_DIR) يجب أن تكون هذه المعلمة فارغة تماماً. استخدامها يتيح للمستخدمين (حتى غير ذوي الصلاحيات العالية) قراءة أو كتابة ملفات على نظام تشغيل الخادم، وهو تكتيك كلاسيكي لزرع البوابات الخلفية.

(في الإصدارات الحديثة، استُبدلت هذه التقنية باستخدام Directory Objects الصارمة).

إلغاء المصادقة الضعيفة عن بُعد:(REMOTE_OS_AUTHENT)

Ahmed Abdelfatah

يجب تعيينها إلى FALSE. إذا كانت TRUE ، فإن قاعدة البيانات ستثق تماماً بنظام التشغيل الخاص بالعميل (Client) لإجراء المصادقة، مما يتيح للمهاجمين انتحال شخصيات إدارية بسهولة بمجرد تزوير اسم المستخدم على أجهزتهم المخترقة.

تقييد قاموس البيانات:(O7_DICTIONARY_ACCESSIBILITY)

يجب تعيينها إلى FALSE بلا مساومة. إذا تُركت TRUE ، فإن أي مستخدم يمتلك صلاحية SELECT ANY TABLE سيتمكن من قراءة جداول النظام الأساسية الحساسة جداً (مثل SYS.USER$ التي تحتوي على تجزئات كلمات المرورPassword Hashes ، مما يعرض النظام لهجمات كسر كلمات المرور(Cracking)

٣,٥ تحصين الشبكة ومستمع أوراكل(Oracle Listener & Network)

في ظل تطور تكتيكات اعتراض الشبكات (MITM) وبرمجيات فحص الذاكرة Memory) (Scraping، أصبح تشفير البيانات أثناء النقل (Data-in-Transit) بنفس أهمية تشفيرها أثناء السكون(Data-at-Rest)

فرض التشفير الأصلي للشبكة (Native Network Encryption - NNE) أو:TLS 1.3

يجب عدم السماح بأي اتصالات غير مشفرة (Clear-text) بين التطبيقات وقاعدة البيانات (عبر المنفذ ١٥٢١ الافتراضي). سواء كنت تستخدم (NNE) عبر إعدادات sqlnet.ora ، أو تعتمد شهادات(TLS) ، يجب فرض التشفير ليصبح "مطلوباً (REQUIRED) "وليس "مقبولاً " .(ACCEPTED) هذا يحبط محاولات المجموعات الاستخباراتية لالتقاط بيانات الاعتماد المارة في الشبكة.

الحماية من تسميم المستمع (Listener Poisoning) وتقييد العقد(VNCR)

المستمع (Listener) هو البوابة الأولى. المهاجم الخبير سيحاول تسجيل خدمة وهمية (Fake Service) لدى المستمع لتحويل حركة المرور الصالحة إلى خوادمه المارقة.

لإحباط ذلك، يجب تفعيل التحقق من العقدة الصالحة للتسجيل (Valid Node Checking for Registration - VNCR) في ملف listener.ora تضمن هذه الميزة أن المستمع سيرفض

Ahmed Abdelfattah

أي طلب لتسجيل خدمة قاعدة بيانات جديدة إلا إذا كان قادماً من عناوين (IP) محددة وموثوقة مسبقاً (مثل خوادم قاعدة البيانات الشرعية فقط).

٣,٦ التخلص من كلمات المرور المحلية ودمج الهوية (Identity Weaponization Defense)

نظراً لأن المجموعات الهجومية المتقدمة تعتمد بكثافة على هجمات تجاوز المصادقة وسرقة الجلسات(Identity Weaponization) ، يجب على المؤسسات التوقف الفوري عن إدارة حسابات قاعدة البيانات بشكل مستقل ومحلي. لصد الهجمات الآلية وهجمات إرهاق المصادقة (MFA Fatigue) ، يجب تطبيق التالي:

- **المستخدمون المدارون مركزياً :(Centrally Managed Users - CMU)**

يجب ربط قواعد بيانات أوراكل بأنظمة الهوية المؤسسية المركزية مثل Microsoft Active Directoryأو Azure AD هذا الدمج يضمن عدم بقاء أي حسابات "خاملة (Dormant Accounts) " في قاعدة البيانات بعد مغادرة الموظفين للشركة، ويتيح في الوقت ذاته تطبيق سياسات المصادقة متعددة العوامل (MFA) المقاومة للتصيد بشكل مركزي وصارم قبل السماح لأي اتصال بالوصول إلى الشبكة أو قاعدة البيانات.

- **ملفات تعريف المستخدمين:(Password Profiles)**

كخط دفاع أخير في حال فشل الأنظمة المركزية، يجب برمجة ملفات تعريف قاعدة البيانات للرد على الهجمات:

التقييد الصارم لمحاولات الدخول :(FAILED_LOGIN_ATTEMPTS) خفض عدد المحاولات الفاشلة المسموح بها (إلى ٣ أو ٥ كحد أقصى) يوقف هجمات التخمين (Brute-force) في ثوانٍ.

دوال التحقق من التعقيد :(Password Verification Functions) ربط كافة ملفات التعريف بدالة (PL/SQL Function) تفرض تعقيداً عالياً لكلمات المرور وتمنع إعادة استخدام الكلمات المدرجة في قوائم التهديدات العالمية.

Ahmed Abdelfattah

٣,٧ الخلاصة التشغيلية للـ DBA

تحصين النواة ليس مشروعاً يُنفذ لمرة واحدة، بل هو "حالة تشغيلية" مستمرة.

١. فعل التشفير الشفاف (TDE) وخزنة قاعدة البيانات (Vault) لحماية البيانات حتى في حال سقوط نظام التشغيل.
٢. قم بسحب الصلاحيات المفرطة المباشرة فوراً واستبدلها بأدوار (Roles) مقيدة وقم بتقييد حزم `PUBLIC`
٣. عطل المعلمات التكوينية الخطرة (Parameters) التي عفا عليها الزمن.
٤. افرض التشفير على مستوى الشبكة وقم بتقييد المستمع (Listener) بقوائم بيضاء (White-lists)صارمة، وانتقل لإدارة الهوية مركزياً.

بمجرد إرساء هذه الأساسات الصلبة، يمكننا الانتقال بثقة إلى الفصل القادم لتفعيل "المراقبة الاستباقية والتدقيق الذكي" لاكتشاف المهاجم قبل أن ينفذ ضربته.

Ahmed Abdelfattah