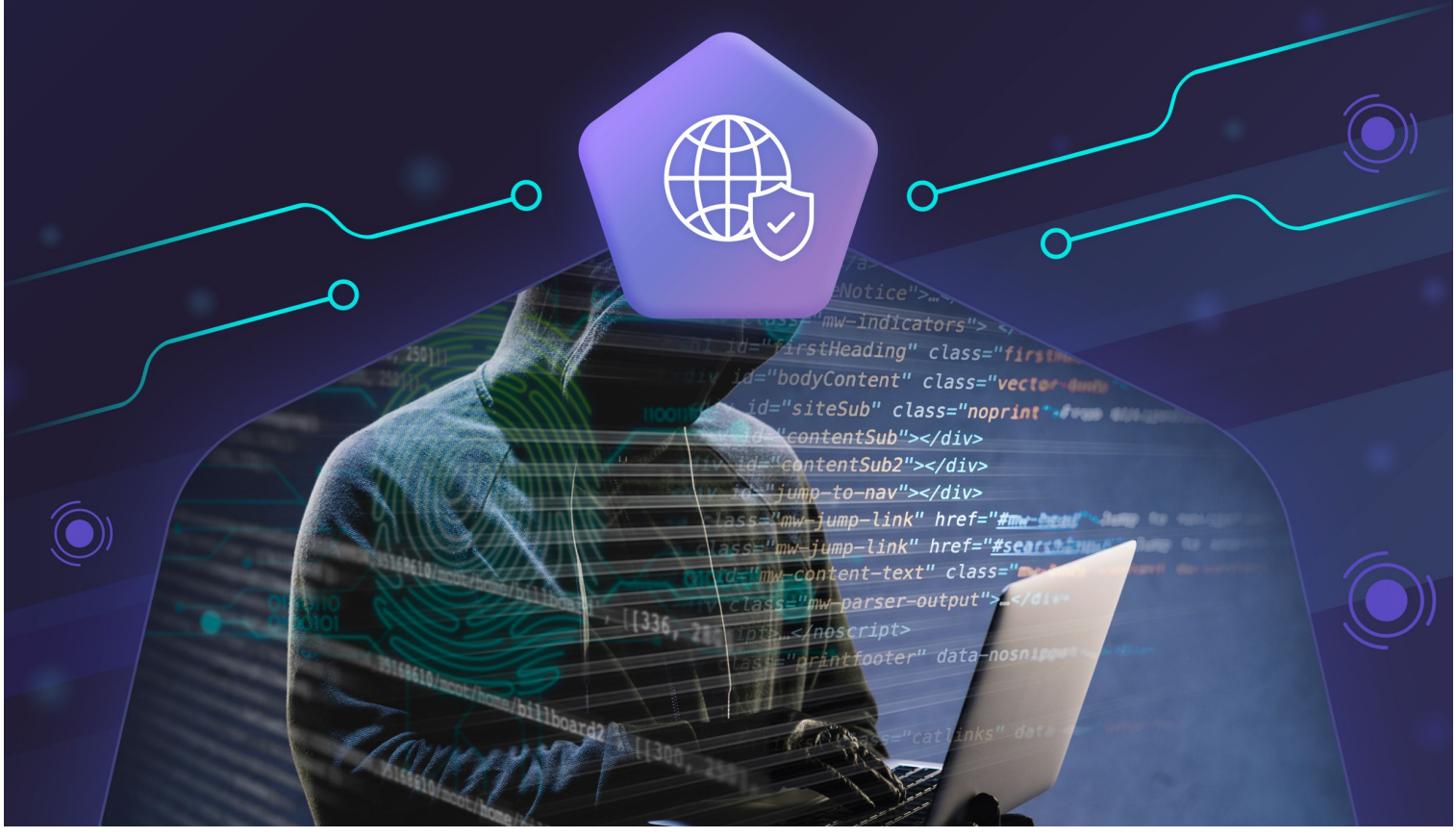
يسر جمعية الدعوة والإرشاد وتوعية
الجاليات بغرب الديرة دعوتكم لحضور

دورة
الأمن السيبراني

مقدم الدورة
أ/ محمد بن إبراهيم الخرجي

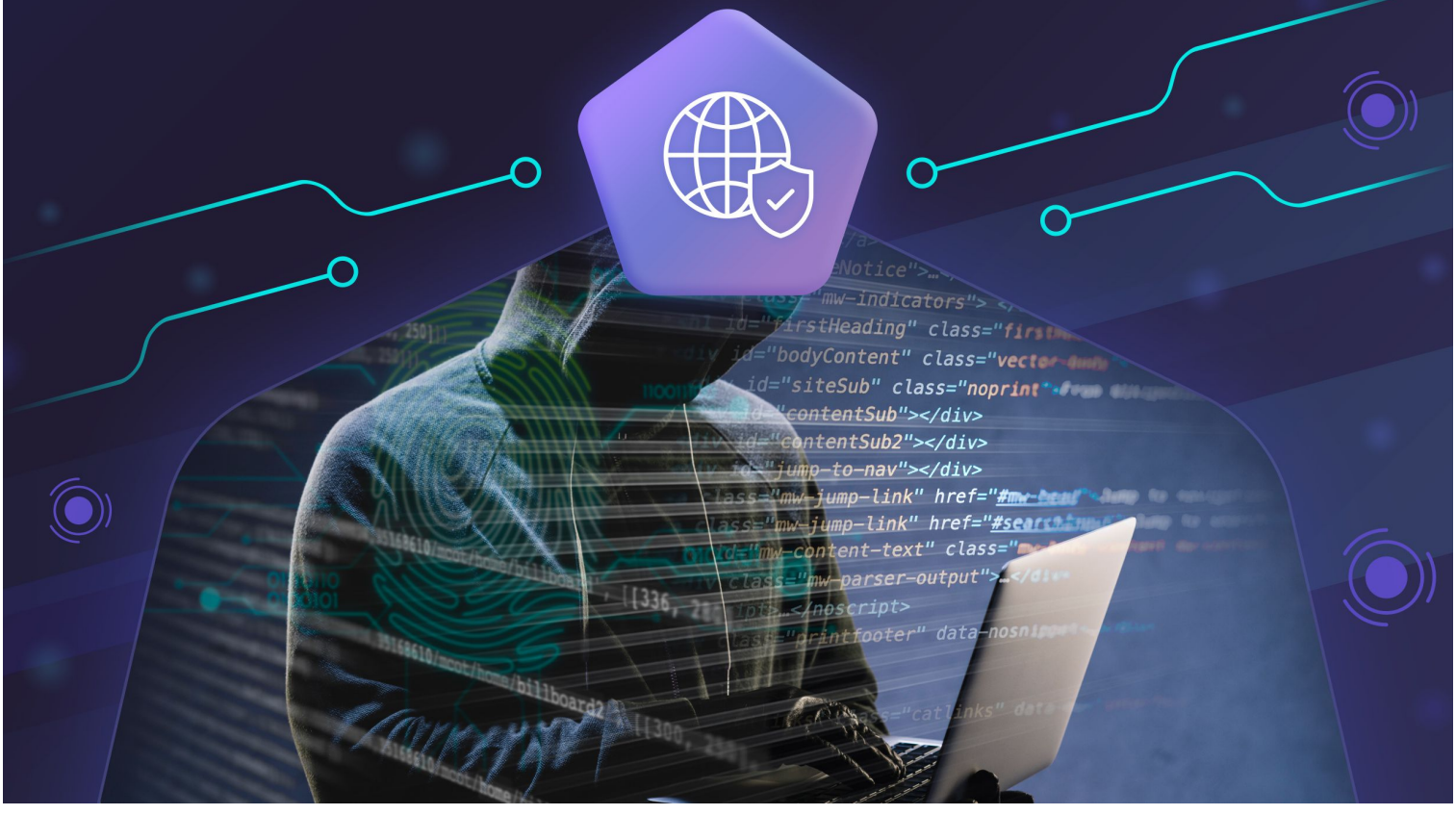
يوم الثلاثاء الموافق 2023/3/21م



دورة
الأمن السيبراني

مقدم الدورة

أ/ محمد بن إبراهيم الخرجي



النقاط الرئيسية:

- تُلحق الجرائم الإلكترونية الضرر بالشركات الكبيرة والصغيرة على السواء، وتبلغ جملة الخسائر الناجمة عنها نحو 100 مليار دولار سنوياً.
- من الأهمية اختيار كلمات مرور قوية تتكون من 14 خانة على الأقل وتتغيّر كل ثلاثة أشهر.
- تظل البيانات غير محصّنة تمامًا من الهجمات حتى بعد بناء جُدر الحماية اللازمة، والسبب هو الجهد البشري الذي ينقصه الكمال.
- الجهل بالأمن السيبراني واللامبالاة والسذاجة في اتخاذ الاحتياطات من أهم عوامل نجاح الجرائم الإلكترونية.
- رغم أهمية الإنفاق على الأمن السيبراني لا بد من دراسة العائد مقابل التكلفة.
- مثلما تخصص المنشآت جزءً من ميزانيتها لتأمين الممتلكات والسيارات يجب أن تخصص ميزانية لتأمين نفسها من المخاطر السيبرانية.
- في بعض الأحيان يكون التصرف الصحيح إزاء الاختراقات هو عدم الاستجابة لمطالب المهاجمين.
- عدم اختصاص المديرون التنفيذيون في الأمن السيبراني لن يمنعهم اتخاذ قرارات سليمة بهذا الخصوص.
- إخفاء خبر الهجمات السيبرانية عن العملاء خطأ كبير على قادة الشركات اجتنابه؛ فالعملاء سيتقبلون الصراحة لكنهم لن يتسامحوا مع التكتّم.

قائمة تدقيق المخاطر:

يشكل القراصنة تهديداً مستمراً على كل الشركات، إذ سبق أن استهدفوا شركات جوجل وسوني وداوكيميكال والحكومة الأمريكية بعينها، بل وهاجموا شركات كبرى مثل كوكاكولا مثلما هاجموا جهات أقل شهرة مثل سلسلة متاجر "شناكس". وبالرغم من أن وسائل الإعلام تركّز في تغطيتها على الشركات الكبيرة فقط، إلا أن الهجمات السيبرانية تستهدف الشركات الصغيرة أيضاً وبأعداد متزايدة. وتبلغ الخسائر الناجمة عن الجرائم السيبرانية أكثر من 100 مليار دولار سنويًا، وهي بذلك تجارةٍ ضخمة. تجارة يتمتع قراصنتها بمعرفة متقدّمة بالتكنولوجيا، علاوة عن كونهم بارعون اجتماعياً وتنظيميّا. وهؤلاء القراصنة يشكلون خطراً على كل نشاط ما دام جزءًا من الاقتصاد الحديث، حيث لا توجد صناعة أو منطقة جغرافية أو ملف تجاري محصن من الهجوم السيبراني.

"كثير من مخاطر عصرنا السيبراني هي نفسها المخاطر القديمة لكنها تختلف فقط في الشكل والطرق والصيغ والوسائل."

نقاط الضعف التي يستغلها المخترقون:

الملكية الفكرية والأسرار التجارية: لا تحتفظ بالمعلومات الحساسة على حاسوبك، واحرص على ابقائها بعيدة عن الهواتف المحمولة. فالأسرار تكون أكثر أماناً عند حفظها في مكان غير متصل بالإنترنت أو حفظها بالطريقة التقليدية مثل الأوراق.

المنافسون : عادةً ما يخوض منافسوك التحدي بشرف، ولكن قد يقوم بعضهم من عديمي المبادئ بتوظيف الجواسيس لسرقة أسرار منشأتك، فانتبه.

حفظ البيانات على الحاسوب: مجرد حفظ السجلات والبيانات على أجهزة الحاسوب يؤدي إلى خلق نقاط ضعف وثغرات.

الوصول إلى الإنترنت: على الرغم مما يتوفر من جدران الحماية (firewall) والتشفيرات وغيرها من أساليب التأمين، تظل أنظمتك الداخلية على بعد خطوة واحدة فقط من الاختراق إذا كانت متصلة بالإنترنت.

منافذ "USB": تخلق منافذ "USB" نقاط ضعف أمنية، وقد اتضح ذلك من هجوم دودة "ستوكسنت" الحاسوبية الخبيثة التي تصيب نظام الويندوز.

أقراص "DVD" وأقراص "CD": ربما تكون قد نسيت أجهزة التخزين هذه التي كانت تستخدم قديماً، ولكن لم ينساها لصوص البيانات! حيث استخدم الجندي الأمريكي "برادلي مانينغ" قرص "CD" لاختراق جدار الحماية العسكري لنقل معلومات سرية إلى موقع "ويكيليكس."

حفظ البيانات في مكان خارجي: يمّكنك تخزين معلوماتك لدى طرف ثالث من الاستمرار في العمل في حالة وقوع كارثة طبيعية أو هجوم إرهابي، ومع ذلك فإنه يعرضك لخطر انتهاك البيانات من الطرف الثالث نفسه.

تلقيم البيانات: هي وسيلة لتلقي البيانات المحدثة من مصادر البيانات المختلفة، حيث تنشر المؤسسات المالية وتجار التجزئة في التجارة الإلكترونية كميات هائلة من البيانات بسرعات عالية، وهذا أمر ضروري نظراً لطبيعة عملهم، ولكنه يخلق نقاط ضعف وثغرات.

"من مسؤولياتك الأساسية بصفتك مديراً أن تتحكم في المخاطر لتحمي عملك وتخلق بيئة آمنة للنمو والازدهار."

تحاول الجهود المستمرة المبذولة في قطاع التكنولوجيا تقليل أضرار تهديد القرصنة المتزايد، ومن الأمثلة البارزة على ذلك إصدار شركة "مايكروسوفت" تحديثين أمنيين كل ثلاثاء من الأسبوع الثاني من كل شهر، حيث يتيح "تحديث الثلاثاء الأمني" للعاملين في مجال تكنولوجيا المعلومات تحصين أنظمتهم ضد التهديدات الأمنية. وإذ تقع مسؤولية تحقيق الأمن السيبراني على عاتق المؤسسات الفردية ومديريها، فالأمر متروك لك للتعرف على التهديدات التي تتعرض لها مؤسستك. وتتمثل مسؤوليتك بالتحديد في توظيف خبراء في تكنولوجيا المعلومات لتولّي مهمة تأمين منشأتك، إضافة إلى تدريب الموظفين على فهم مخاطر القرصنة وكيفية تجنبها.

كلمات مرور يصعب التنبؤ بها واختراقها:

لغايات احترازية، اختر كلمات مرور أكثر أماناً لشركتك. وتتكون كلمات المرور القوية من أربعة عشر خانة أو أكثر، وتشمل على الأقل على حرفين كبيرين وحرفين صغيرتين ورقمين ورمزين من الرموز الخاصة (مثل @/#/$/%).

"لا يمكنك تحويل البسطاء إلى أذكياءً، لكن يمكنك زيادة وعيهم." (جون فيري، خبير سيبراني")

لكن، لا تعتقد أن مجرد اضافة رمز إلى كلمة المرور سيجعلها غير قابلة للاختراق. ينبغي أن تعلم أن القراصنة يستخدمون برامج تخمّن الآلاف من كلمات المرور، وأنهم يقومون ببحثٍ كافٍ على وسائل التواصل الاجتماعي لتحديد أسماء أفراد عائلتك والفرق الرياضية المفضلة لديك وكل ما من شأنه تحديد كلمة مرورك. وعليك ألّا تعيد استخدام كلمات المرور القديمة، وأن تغيّر كلمات المرور كل ثلاثة أشهر. وإذا وقعت منشأتك ضحية القراصنة فتأكد من قيام الجميع بتغيير كلمات المرور الخاصة بهم وخاصة مسؤولي النظام.

اجتنب الأخطاء الفادحة:

بالرغم من كون جدار الحماية (**firewall**) حائط منيع لحماية بياناتك، تظل حمايتك عرضة للتقصير البشري. ويجب أن تعلم أن إدارة هذه "المخاطر البشرية" هي مسؤوليتك. وعليك الحذر من هجمات "التصيد الاحتيالي" لأنها شائعة وتتمثل في رسائل بريد إلكتروني مفخخة بالبرامج الحاسوبية الضارة. كما يستخدم القراصنة "التصيُّد بالرمح"، وهو إرسال رسائل بريد إلكتروني معدّة بدقة إلى شخص معين أو مجموعة مقصودة للحصول على نتائج دقيقة. لذا احذر من استخدام القراصنة هذا الأسلوب لحث الموظفين على تنزيل برامج ضارة على حواسيبهم. ويجب أيضاً أن تنتبه إلى أن الرسائل الزائفة تبدو صحيحة للوهلة الأولى، لذا درّب موظفيك على أن يطرحوا ثلاثة أسئلة على أنفسهم قبل فتح أي رسالة ذات مرفق: هل هذه الرسالة ذات صلة بما أقوم به؟ هل كنت في انتظار هذه الرسالة من أحدهم؟ هل المرسل جهة رسمية أو شخصية معروفة؟ عموماً، ثقّف موظفيك حول مخاطر البريد الإلكتروني ووسائل التواصل الاجتماعي، وكن على علم أن القراصنة في بعض الحالات يرسلون فواتير مزيفة ويتحدثون بإقناع عبر الهاتف.

إضافة إلى ما سبق، اجتنب هذه الأخطاء الفادحة:

الجهل: قد يجهل الموظفون مخاطر الأمن السيبراني ولا يعرفون قواعدك وسياساتك للحد من تلك المخاطر، وفي هذه الحالة يمكنك معالجة هذا النقص عن طريق تدريبهم.

اللامبالاة: قد يدرك موظفوك المخاطر ويعرفون سياساتك، ولكن لا يتبعون الإجراءات الأمنية المعمول بها. ومن علامات عدم مبالاتهم فشلهم في اكمال في إكمال تدريبات الأمن السيبراني وتجاهلهم قواعد الأمان.

السذاجة: حتى الأذكياء يقومون بتصرفات ساذجة أحيانًا! وتبين ذلك من خلال تجربة أجريت في منشأة حكومية أمريكية، حيث وضع الباحثون ذاكرات "USB" متنقلة في ساحة اصطفاف السيارات وانتظروا ليروا ما سيحدث، قام الموظفون بالتقاطها وإدخال 60٪ منها في الحواسيب الحكومية، على الرغم من القواعد التي تحظر مثل هذه الأعمال تحديداً.

الفضول: تستغل هجمات "التصيد الاحتيالي" الفضول البشري، وتدّعي مثلًا تقديم معلومات حول وجود مشكلة في حساب مصرفي يخص المستهدف بالرسالة.

ضعف القيادة: خذ الأمن السيبراني على محمل الجد. إذا كنت مديراً مهماً، فيجب عليك حضور الدورات التدريبية، وأحرص على أن يدرك موظفوك أهمية الأمن السيبراني.

عدم المساءلة: هل يتجاهل موظفوك السياسات الأمنية؟ إذا كان الأمر كذلك، افرض عليهم العقوبات، فإذا لم تحاسب أي شخص على أخطائه سيستمر سلوكهم المحفوف بالمخاطر.

التعامل مع المخاطر:

لديك أربع خيارات للتعامل مع خطر الهجمات السيبرانية، اختّر من بينها وفقاً لوضعك الحالي وما يتوفر لمنشأتك من قدرات تقنية وما يحدّق بها من مخاطر:

1. **تقليل المخاطر:** قد يكون الإنفاق على سد ثغرات دفاعاتك هو الخطة التأمينية الأكثر جدوى، لكن لا تتسرع في هذه الخطوة دون مقارنة العائد مقابل الإنفاق. إذ كثيراً ما تنفق الشركات الملايين في تكنولوجيا المعلومات لتأمين معلومات لا تصل قيمتها إلى نصف المبلغ المنفق، لذا اطرح على نفسك ثلاثة أسئلة عند الإقدام على وضع ميزانية الأمن السيبراني: كيف يمكنني التقليل من هذه المخاطر؟ وكم ستكون التكلفة؟ وكم من الوقت ستستغرق؟
2. **إحالة المخاطر (تأمين المخاطر):** أوكل مخاطر هجوم الأمن السيبراني إلى جهة معنية لتتولى مسؤوليتها، مثلما توكل مخاطر ممتلكاتك وسياراتك إلى شركات التأمين. وقد تنامى سوق التأمين السيبراني وتجاوزت قيمته مليار دولار، وأصبحت له وثائق تأمين وسياسات تأمينية معروفة تغطي مسؤولية الطرف الثالث عن الأضرار الناجمة عن الخرق بالإضافة إلى تكاليف إدارة الأزمات للطرف الأول مثل تكاليف عمليات التحقيق وتكاليف الإجراءات القانونية وتكاليف موظفي مركز الاتصال.
3. **تقبُّل المخاطر:** يكون التصرف الصحيح في بعض الأحيان ضد التهديد الأمني هو تجاهله. إذ ربما تكون مخاطرك قليلة أو قد تكون قيمة بياناتك ليست عالية. في كل مرة تتعرّض منشأتك إلى هجوم ما عليك إلا تقدير الأضرار ومن ثم سيتبيّن لك إن كان التجاهل هو التصرّف الأنسب.
4. **تجنّب المخاطر:** قد تكون المعدات القديمة والبرامج القديمة مليئة بالثغرات الأمنية، لذا ينبغي عليك تحديث الأجهزة والبرامج لتقلل منها. فالتصرف المنطقي هو تجنب المشكلة من البداية عبر استبدال النظام القديم وشراء خوادم وبرامج جديدة أكثر أماناً. ومن طرق تجنب المخاطر عدم إدراج المعلومات الشخصية في السيرة الذاتية الرسمية وإزالة أسماء أطفالك ومعلوماتك سكنك من أي سيرة ذاتية منشورة.

أفضل ممارسات الأمن السيبراني:

على الرغم من أن لكل منشأة تدابير وقائية خاصة تناسب مجال عملها، إلّا أن التدابير التالية مفيدة لفئة كبيرة من الأنشطة:

توطين سياسات الأمن السيبراني: درّب جميع العاملين على فهم هذه السياسات وممارستها بانتظام.

ضبط إعدادات البرامج ومواكبة التحديثات: استخدم فقط النسخ المعتمدة والمختبرة من أنظمة التشغيل وبرمجيات مكافحة الفيروسات.

إعداد اتصالات حدودية وأنظمة كشف تسلل قوية: استعن بطرف ثالث مستقل ليختبر بانتظام قابلية أنظمتك للاختراق.

رفض الكل والسماح للاستثناءات: يجب أن تكون سياستك الافتراضية هي رفض وصول الجميع إلى الشبكة إلا بإذن؛ لتصفية الحركة على الشبكة وحظر أي زوار غير مرغوبين.

إعداد تسلسل هرمي للامتيازات (تخصيص الأذونات): السماح للمستخدمين بالوصول إلى المعلومات والخدمات التي يحتاجون إليها فقط؛ لإحباط محاولات الذين يزوّرون الهويات لسرقة معلومات حساسة.

تشفير كل شيء: تشفير بيانات حاسوب المنزل وحواسيب المكتب والبيانات المتنقلة، وتشفير محركات الأقراص الثابتة على أجهزة الحاسوب المكتبية والمحمولة وغيرها من الأجهزة.

تثبيت نظام لاكتشاف الاختراقات: يمكنك اكتشاف الانتهاكات الداخلية والهجمات الخارجية وإيقافها على الفور من خلال عمليات المسح الداخلية والخارجية الدقيقة.

- **إدراج الأمن السيبراني ضمن أولويات الشركة:** امنع استخدام محركات قراءة أقراص "USB" وأجهزة قراءة أقراص "CD"، واسمح باستخدمها ضمن ظروف خاضعة للرقابة. وعند استيراد البيانات وتصديرها قم بتنفيذ "سياسات الامتثال للاتصال"، والتي هي عبارة عن خمس خطوات حاسمة وضعتها وزارة الدفاع الأمريكية للدفاع عن المنظمات من الهجمات الإلكترونية وتخفيف المخاطر، وكذلك لا تسمح بالوصول إلى الشبكة عن بعد إلا في الظروف الخاضعة للرقابة فقط.

استثمر في موظفي تكنولوجيا المعلومات: كلما زادت مخاطرك زادت الأولوية التي يجب أن توليها لموظفي تكنولوجيا المعلومات لديك، واشتدت حاجتك للاستعانة بخبراء في تكنولوجيا المعلومات ممن حصلوا على التدريب والشهادات المناسبة.

إبقاء بيانات العمل المهمة بعيدة عن الإنترنت: بعض بياناتك مثل المراسلات العامة ليست ذات قيمة مهمة، ولكن بيانات الملكية الفكرية والأسرار التجارية الخاصة بك لها قيمة عظيمة وعليك تداولها خارج الإنترنت.

إدراك المخاطر:

قـادة المنشـآت ليسـوا بحاجـة إلـى أن يكونـوا خبـراء حتـى يتخـذوا قـرارات فعّالـة، ومـا عليهم إلا إثارة هذه الأسئلة ليتبيّن لهم الإجراء اللازم:

مـا هـي تهديـدات أمننـا؟ يتطـور مجـال الأمـن السـيبراني باسـتمرار، لـذا ينبغـي إعـادة فحص نقاط ضعفنا وثغراتنا يومياً.

ما مدى فعالية أنظمتنا؟ إعداد مقاييس أداء لقياس مدى هشاشة أمننا السيبراني.

ما مـدى ضعفنـا؟ قـد تعمـل أنظمـة تكنولوجيـا المعلومـات لديـك بكفـاءة، ولكـن هـذا لا يعني أنها آمنة تمامًا.

هـل لدينـا الموظفيـن المناسـبين؟ هـل تـم تدريبهـم جيّـدًا؟ وهـل يتبعـون الإجـراءات المناسـبة حيـث يعـد الخطـأ البشـري تهديـداً خطيـراً حتـى لشـبكة تكنولوجيـا المعلومـات الآمنة.

هـل أنفـق المبلـغ المناسـب علـى الأمـن السـيبراني؟ يختلـف مبلـغ الإنفـاق المناسـب باختلاف المنشآت، لكن الإنفاق على التدريب والأجهزة والبرمجيات بنود ضرورية.

هجوم الاختراق:

كن متأهّبًا للتصرّف ضد الهجمات حتى قبل وقوعها، واهتم جيّدًا بالرأي العام حتى لا تقع في نفس خطأ شركة سوني عندما تصرّفت بسذاجة إثر هجوم عام 2001م الذي اخترق شبكة "بلاي ستيشن" إذ أصدرت الشركة بياناً مقتضباً متأخراً غير مطمئن حول تسرّب بيانات بطاقات ائتمان المشتركين، في وقت كانت الهواجس تعصف بهم لأيام دون رد من الشركة. ومثال آخر على أخطاء التصرّف هو ما فعلته سلسلة المتاجر "شناكس" عندما اخترق نظامها في العام 2013م إذ رفض مسؤولو الشركة التحدث إلى وسائل الإعلام وقدموا بيانات مكتوبة فقط وتأخر ردّ الرئيس التنفيذي إلى أن فات الأوان فرُفعت على السلسلة دعاوى جماعية من العملاء.

لذا، الإدارة التخطيط لمقابلة الهجمات السيبرانية كما تخطط للكوارث الطبيعية تماماً، مع اتّباع الخطوات التالية بعد أي هجوم:

تواصل على الفور: قد يتفهم العملاء مكاشفتهم بتعرضهم للاختراق، ولكنهم لن يكونوا متسامحين عند إخفاء أمر الهجوم عنهم.

استعن باختصاصي علاقات عامة: موظفو العلاقات العامة في منشأتك يكونون عادة غير معتادين على التعامل مع ظروف الهجمات السيبرانية، لذا هناك حاجة للاستعانة باختصاصيين خارجيين عند الأزمات.

ضع كبار المسؤولين أمام الكاميرات: قد تنجح في إصدار تصرفات ميدانية فعالة ضد الهجمات السيبرانية، ولكن إذا واصلت الامتناع عن الظهور الإعلامي، فسيظن العملاء أنك لا تهتم بمخاوفهم. وعليه، حث المسؤوليك في شركتك على التعامل مع وسائل الإعلام.

كن كريماً: قدّم تعويضاً للعملاء لمساعدتهم على التغاضي عن الانتهاك الذي تعرضت له معلوماتهم، واعلم أن ذلك مهما كلفك في الحاضر سيوطد علاقتك بهم على المدى الطويل.

قائمة بأسماء المشاركين
في دورة الأمن السيبراني

١	إبراهيم بن أحمد الزيلعي
٢	مبارك بن سالم الزهراني
٣	علي بن صالح الجار الله
٤	علي بن محمد العنزي
٥	أحمد بن إبراهيم الزيلعي
٦	مزيد بن هادي مقلعب
٧	عبد الله بن علي الحميدي
٨	خالد بن إبراهيم العقيفي

جمعية الدعوة و الإرشاد
وتوعية الجاليات بغرب الديرة

جمعية الدعوة الإرشاد وتوعية الجاليات بغرب الديرة

رقم الحساب العام : SA0580000195608010220007

01143919 42-01143503 62 | 0 1 1 4 3 9 1 8 5 1

ص.ب: 154488 رمز بريدي: 11736 | @ D e r a d a w a 1

جـمعيـة الـدعـوة و الإرشـاد
وتوعية الجاليات بغرب الديرة

يسر جمعية الدعوة والإرشاد وتوعية
الجاليات بغرب الديرة دعوتكم لحضور

دورة
مكافحة الإرهاب

مقدمة
د/ عبد الله بن حمد القعيد

يوم الخميس الموافق 2023/9/27م

قائمة بأسماء المشاركين

في دورة مكافحة الإرهاب

١	محمد بن إبراهيم الخرجي
٢	إبراهيم بن أحمد الزيلعي
٣	مبارك بن سالم الزهراني
٤	علي بن صالح الجار الله
٥	عبد الله قحطان
٦	مزيد بن هادي مقلعب
٧	خالد بن إبراهيم العقيفي
٨	حافظ فضل ربي
٩	علي بن محمد العنزي
١٠	عبد الله بن علي الحميدي
١١	عبد الرزاق نيلي برمبان
١٢	محمد عبد الرب عفان
١٣	صالح خيري العربي
١٤	محمد سليم ساجد مدني
١٥	محمد عبد الواسع عبد القيوم

يسر جمعية الدعوة والإرشاد وتوعية
الجاليات بغرب الديرة دعوتكم لحضور

دورة آلية الإبلاغ عن وجود شبهة غسل الأموال وتمويل الإرهاب

مقدمة
د/ بندر بن عبدالعزيز المحيميد

يوم الإثنين الموافق 2023/11/20م
عن بعد

الحضور
أعضاء االلجنة العمومية+ العاملين في الجمعية

جمعية الدعوة و الإرشاد
وتوعية الجاليات بغرب الديرة

جـمعيـة الـدعـوة و الإرشـاد
وتوعية الجاليات بغرب الديرة

يسر جمعية الدعوة والإرشاد وتوعية
الجاليات بغرب الديرة دعوتكم لحضور

دورة خطورة غسيل الأموال

مقدمة
أ/ محمد بن إبراهيم الخرجي

يوم الثلاثاء الموافق 2023/9/11م

جمعية الدعوة و الإرشاد
وتوعية الجاليات بغرب الديرة

دورة خطورة غسيل الأموال

مقدمة
أ/ محمد بن إبراهيم الخرجي

المقصود بغسل الأموال ؟

يعد مرتكباً لجريمة غسل الأموال كل من علم أن الأموال متحصلة من جريمة أصلية وقام عمداً بأي مما يلي :

-**تحويل متحصلات** أو نقلها، وذلك بقصد إخفاء المال أو تمويه طبيعته أو مصدره أو مكانه أو صاحبه أو صاحب الحق فيه أو تغيير حقيقته أو الحيلولة دون اكتشاف ذلك أو عرقلة التوصل إلى مرتكب الجريمة الأصلية.

-**اكتساب المتحصلات** أو حيازتها أو استخدامها أو إدارتها أو حفظها أو استبدالها أو إيداعها أو ضمانها أو استثمارها أو التلاعب في قيمتها أو إخفاء أو تمويه الطبيعة الحقيقية لها أو لمصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها.

كيف يتم غسل الأموال ؟

تحـدث عمليـة غسـل الأمـوال مـن خلال ثلاثـة مراحـل هـي الإيداع، والتمويه والدمج.

ما هي الاثار السلبية لعمليات غسل الاموال ؟

على الرغم من أن البعض قد يرى أنه لا فرق بين الأموال القذرة والأموال النظيفة وأن الأموال القذرة تستطيع أن تساعد في دفع عجلة التنمية في دولة ما إلا أنه من الواضح أن اللجوء إلى الأموال القذرة يترتب عليه عدة نتائج :سلبية، يتمثل أهمها فيما يلي:

1. الآثار الاقتصادية

- إضعاف قدرة السلطات على تنفيذ السياسات الاقتصادية بكفاءة.
- التضخم وارتفاع المستوى العام للأسعار
- إضعاف استقرار سوق الصرف الأجنبى.
- وجود خلل فى توزيع الموارد والثروة داخل الاقتصاد.
- توجيه الموارد نحو الاستثمارات غير المجدية على حساب الاستثمارات المجدية التى تسهم فى التنمية.
- تهديد الاستقرار المالى والمصرفى.
- تهديد استقرار البورصات وإمكانية انهيارها.

2. الآثار السياسية

- انتشار الفساد السياسى والإداري واستغلال النفوذ.
- الإضرار بسمعة الدولة، وبخاصة لدى المؤسسات المالية الدولية.
- نفاذ المجرمين الى مناصب سياسية هامة بالدولة.
- استغلال الأموال المغسولة فى تمويل الارهاب

3. الآثار الاجتماعية

- وجود تفاوت بين الطبقات الاجتماعية.
- صعود فئات اجتماعية دنيا إلى أعلى الهرم الاجتماعى.
- انتشار الفساد الوظيفى والرشوة وشراء الذمم.
- عدم خلق فرص عمل حقيقية مما يؤدى إلى تفاقم مشكلة البطالة وتدنى الأجور للأيدي العاملة وتدنى مستوى المعيشة .

قائمة بأسماء المشاركين

في دورة خطورة غسيل الأموال

١	إبراهيم بن أحمد الزيلعي
٢	مبارك بن سالم الزهراني
٣	علي بن صالح الجار الله
٤	عبد الله قحطان
٥	أحمد بن إبراهيم الزيلعي
٦	مزيد بن هادي مقلعب
٧	فواز بن عبد الله إمام
٨	خالد بن إبراهيم العقيفي
٩	علي بن محمد العنزي
١٠	عبد الله بن علي الحميدي
١١	عبد الرزاق نيلي برمبان
١٢	محمد عبد الرب عفان
١٣	صالح خيري العربي

جمعية الدعوة و الإرشاد

وتوعية الجاليات بغرب الديرة

جمعية الدعوة الإرشاد وتوعية الجاليات بغرب الديرة

رقم الحساب العام : SA0580000195608010220007

0114391942-0114350362 | 0 1 1 4 3 9 1 8 5 1

@ D e r a d a w a 1 | ص.ب: 154488 رمز بريدي: 11736