SJST
sjst.scst.edu.ly

Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)

مجلة صرمان للعلوم والتقنية
Vol7, No.1, Jan-Jun. 2025
Pages: 240 ~ 249

الجرائم الإلكترونية المرتبطة بالإنترنت المظلم وتأثيرها على البيانات المحاسبية

مفيدة ضو الهواري[1]، محمد الطاهر صقر[2]، حنان الشيباني خليفة[3]، سهيلة جمعة خليفة[4]

قسم العلوم الادارية والمالية، كلية صرمان للعلوم والتقنية - ليبيا

*Corresponding author, e-mail: m_hawari@scst.edu.ly

ملخص

تهدف هذه الدراسة إلى تسليط الضوء على الجرائم الإلكترونية المرتبطة بالإنترنت المظلم وتأثيرها على البيانات المحاسبية، حيث يعتبر الإنترنت المظلم بيئة خصبة للأنشطة الإجرامية التي تتضمن سرقة البيانات والتزوير المالي والابتزاز الإلكتروني. تستعرض الدراسة مفهوم الإنترنت المظلم وخصائصه وأبرز الجرائم التي تتم من خلاله، مع التركيز على كيفية استهداف البيانات المحاسبية الحساسة للشركات والمؤسسات.

كما تناقش الدراسة التأثيرات السلبية لهذه الجرائم على نزاهة البيانات المحاسبية ودقة التقارير المالية وثقة المستثمرين وأصحاب المصلحة. يتم التطرق أيضا إلى أهم التدابير الوقائية والتقنيات الحديثة لمكافحة هذه الجرائم، مثل تعزيز الأمن السيبراني واستخدام التشفير والذكاء الاصطناعي.

وتبرز الدراسة أهمية التعاون بين الحكومات والمؤسسات لتعزيز التشريعات التي تحارب الجرائم الإلكترونية على الإنترنت المظلم وتضمن حماية البيانات المحاسبية، مما يساهم في تقليل المخاطر وتأمين بيئة رقمية آمنة للشركات.

Abstract

This study aims to shed light on cybercrimes associated with the dark web and their impact on accounting data. The dark web is a fertile ground for criminal activities, including data theft, financial fraud, and cyber extortion. The study explores the concept of the dark web, its characteristics, and the most prominent crimes conducted through it, focusing on how sensitive accounting data of companies and organizations are targeted.

The research discusses the negative impacts of these crimes on the integrity of accounting data, the accuracy of financial reports, and the trust of investors and stakeholders. It also examines key preventive measures and modern technologies to combat such crimes, including strengthening cybersecurity, utilizing encryption, and employing artificial intelligence.

The study highlights the importance of collaboration between governments and organizations to enhance legislation that combats cybercrimes on the dark web and ensures the protection of accounting data, thereby reducing risks and securing a safe digital environment for businesses.

الكلمات المفتاحية: الجرائم الإلكترونية، الإنترنت المظلم، البيانات المحاسبية، الأمن السيبراني، التشريعات القانونية .

1. المقدمة:

تزايدت أهمية البيانات المحاسبية في العصر الرقمي الحالي باعتبارها جزءا أساسيا من القرارات الإدارية والمالية للشركات والمؤسسات. ومع التطور السريع في التكنولوجيا، ظهرت تحديات جديدة تهدد أمن هذه البيانات، من بينها الجرائم الإلكترونية التي تنفذ عبر الإنترنت المظلم [1]. يعد الإنترنت المظلم مساحة رقمية غير مرئية لمحركات البحث التقليدية ويستخدم غالبا لأغراض غير قانونية مثل بيع البيانات المسروقة والتزوير المالي والابتزاز الإلكتروني [2].

تنبع أهمية هذه الدراسة من الحاجة إلى فهم كيفية تأثير الجرائم الإلكترونية المرتبطة بالإنترنت المظلم على البيانات المحاسبية، لا سيما في ظل زيادة اعتماد المؤسسات على التقنيات الرقمية لتخزين ومعالجة بياناتها [3]. تهدف الدراسة إلى توضيح المخاطر التي يفرضها الإنترنت المظلم على سلامة البيانات المحاسبية وتحديد أهم التدابير الوقائية لمواجهتها.

تشير الدراسات إلى أن الجرائم الإلكترونية التي تستهدف البيانات المحاسبية، مثل سرقة التقارير المالية أو التلاعب بها، تؤدي إلى خسائر مالية كبيرة للشركات وتؤثر على سمعتها وثقة المستثمرين فيها [4]. وبذلك تهدف الدراسة إلى تسليط الضوء على

SJST
sjst.scst.edu.ly
Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol7, No.1, Jan-Jun. 2025
Pages: 240 ~ 249

أهمية تعزيز الأمن السيبراني ورفع الوعي حول هذه المخاطر لضمان حماية البيانات المحاسبية ودعم استقرار الأعمال في البيئة الرقمية.

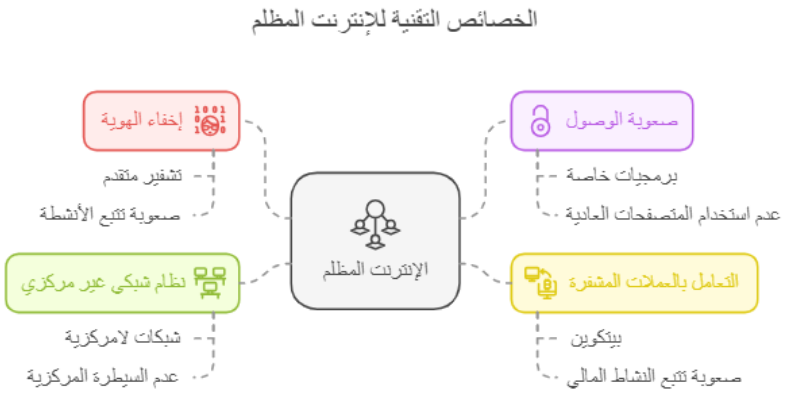
2. الإنترنت المظلم: المفهوم والخصائص

1.2. تعريف الإنترنت المظلم والفرق بينه وبين الإنترنت العادي والإنترنت العميق:

الإنترنت المظلم (Dark Web) هو جزء صغير من الإنترنت لا يمكن الوصول إليه باستخدام محركات البحث التقليدية أو المتصفحات العادية. يعد الإنترنت المظلم فرعا من الإنترنت العميق(Deep Web) [5]. وهو الجزء الأكبر من الإنترنت الذي لا يتم فهرسته في محركات البحث العادية ويشمل قواعد البيانات والحسابات الشخصية والمعلومات المحمية. بينما يتيح الإنترنت العادي (Surface Web) الوصول المفتوح للمحتوى المفهرس والمتاح لعامة المستخدمين، يظل الإنترنت المظلم بيئة مغلقة تحتاج إلى برامج وأدوات متخصصة للوصول إليها. يتم استخدام الإنترنت المظلم في كثير من الأحيان لأغراض غير قانونية مثل بيع المخدرات والأسلحة والبيانات المسروقة [6].

2.2. أبرز الخصائص التقنية للإنترنت المظلم:

يبين الشكل 1. التالي رسما توضيحيا لأبرز الخصائص التقنية للأنترنت المظلم



الشكل 1. يبين الخصائص التقنية للإنترنت المظلم

1) إخفاء الهوية :يعتمد الإنترنت المظلم على تقنيات مثل التشفير المتقدم لإخفاء هوية المستخدمين والمواقع، مما يجعل تتبع الأنشطة صعبا للغاية.
2) صعوبة الوصول :يتطلب الإنترنت المظلم برمجيات خاصة ولا يمكن الوصول إليه عبر المتصفحات العادية.
3) التعامل بالعملات المشفرة :يتم استخدام العملات المشفرة مثل البيتكوين لإجراء المعاملات، مما يزيد من صعوبة تتبع النشاط المالي.
4) نظام شبكي غير مركزي :يعتمد الإنترنت المظلم على شبكات لامركزية لا تخضع لسيطرة أي جهة مركزية.

3.2. أدوات الوصول إلى الإنترنت المظلم) مثل متصفح(Tor):

1) متصفح Tor :يعد بوابة رئيسية للوصول إلى الإنترنت المظلم. يقوم Tor (The Onion Router) بتوجيه الاتصالات عبر شبكة معقدة من الخوادم حول العالم، مما يعزز الخصوصية ويخفي هوية المستخدم.
2) متصفح I2P :وسيلة أخرى للوصول إلى الإنترنت المظلم مع تركيز على الخصوصية والسرية.
3) VPN: غالبا ما يتم استخدام شبكات افتراضية خاصة (VPN) قبل الوصول إلى الإنترنت المظلم لضمان حماية إضافية للهوية.

مجلة صرمان للعلوم والتقنية
Surman Journal for Science and Technology
sjst.scst.edu.ly
ISSN: Online (2790-5721) - Print (2790-5713)
Vol7, No.1, Jan-Jun. 2025
Pages: 240 ~ 249

4) تطبيقات التشفير :يتم استخدام أدوات تشفير مثل PGP (Pretty Good Privacy) لضمان أمان الرسائل والمستندات المتبادلة.

على الرغم من استخدام الإنترنت المظلم في بعض الأحيان لأغراض مشروعة يمثل بيئة محفوفة بالمخاطر نظرا للأنشطة غير القانونية التي تتم من خلاله، مما يستدعي دراسة عميقة لتأثيره على المجالات الحيوية مثل البيانات المحاسبية.

3. أنواع الجرائم الإلكترونية في الإنترنت المظلم:

يبسط المخطط التالي فهم أنواع الجرائم الالكترونية في الانترنت المظلم

الشكل 2. يبين نظرة عامة على الجرائم الالكترونية في الانترنت المظلم

1.3. القرصنة وسرقة البيانات:

يعد القرصنة (Hacking) من أكثر الجرائم شيوعًا على الإنترنت المظلم، حيث يقوم القراصنة باختراق الأنظمة الإلكترونية للشركات والمؤسسات بهدف سرقة البيانات الحساسة. وتشمل البيانات المستهدفة:

1) البيانات المحاسبية: مثل الحسابات والتقارير المالية.
2) بيانات العملاء: مثل المعلومات الشخصية وأرقام البطاقات البنكية.
3) المعلومات السرية للشركات: مثل استراتيجيات العمل أو براءات الاختراع.

يتم استغلال هذه البيانات لأغراض ابتزاز أو بيعها على منصات الإنترنت المظلم.

2.3. بيع البيانات المحاسبية المسروقة:

البيانات المحاسبية المسروقة تعد هدفا رئيسيا للأنشطة غير القانونية على الإنترنت المظلم، حيث يتم عرضها للبيع في منتديات ومواقع متخصصة. تشمل هذه البيانات:

1) سجلات الحسابات.
2) تقارير الأرباح والخسائر.
3) معلومات الضرائب والبيانات البنكية للشركات.

تستخدم هذه البيانات لإجراء عمليات احتيال أو استهداف الشركات بطرق متعددة، مثل تقديم عروض تنافسية غير قانونية أو التلاعب بسمعة المؤسسة.

3.3. الابتزاز الإلكتروني والفدية:(Ransomware)

تستخدم برمجيات الفدية كأداة للابتزاز، حيث يقوم المجرمون بإصابة الأنظمة الحاسوبية للشركات بفيروسات تشفر البيانات وتجعلها غير قابلة للوصول.

1) يطالب المهاجمون بفدية مالية تدفع غالبا باستخدام العملات المشفرة لإعادة فك التشفير.
2) يؤثر هذا النوع من الهجمات بشكل مباشر على العمليات المالية للشركات، مما يؤدي إلى خسائر مالية كبيرة وتعطيل الأعمال.
3) الإنترنت المظلم يعد الوسيلة الأساسية لتوزيع برمجيات الفدية وإجراء التفاوض مع الضحايا.

4.3. الاحتيال المالي وغسيل الأموال:

الإنترنت المظلم يستخدم كمنصة لتنفيذ عمليات احتيال مالي وغسيل أموال عبر تقنيات معقدة [7].. تشمل هذه الجرائم:

1) الاحتيال المالي :إنشاء مواقع مزيفة لإجراء معاملات مالية غير قانونية أو سرقة تفاصيل البطاقات الائتمانية.
2) غسيل الأموال :استخدام العملات المشفرة مثل البيتكوين، لإخفاء مصادر الأموال غير القانونية وتحويلها إلى أموال تبدو مشروعة.
3) يتم تقديم خدمات غاسلي الأموال على الإنترنت المظلم، حيث يتم غسل الأموال المستخرجة من الجرائم الإلكترونية أو غيرها من الأنشطة غير القانونية.

4. تأثير الجرائم الإلكترونية على البيانات المحاسبية:

1. سرقة البيانات المحاسبية الحساسة:

تستهدف الجرائم الإلكترونية البيانات المحاسبية الحساسة للشركات، بما في ذلك:

1) بيانات العملاء :مثل الأسماء والعناوين وأرقام الحسابات البنكية.
2) الحسابات المالية :التي تشمل تفاصيل الإيرادات والمصروفات.
3) التقارير المحاسبية :مثل ميزانيات الشركة وتقارير الأرباح والخسائر والتقارير الضريبية.

سرقة هذه البيانات يمكن أن تؤدي إلى تسرب معلومات سرية، مما يعرض الشركة لخسائر تنافسية وقانونية ويضعف سمعتها في السوق.

2. التلاعب والتزوير في البيانات المالية:

من أبرز التهديدات التي تواجه الشركات هو التلاعب أو التزوير في بياناتها المحاسبية بعد اختراق الأنظمة. تشمل هذه الجرائم:

1) إدخال معلومات غير صحيحة في السجلات المالية.
2) حذف أو تعديل بيانات مهمة تؤدي إلى ظهور الشركة في وضع مالي غير حقيقي.
3) استغلال التلاعب في البيانات لتضليل المساهمين أو الجهات التنظيمية.

يؤثر ذلك بشكل كبير على شفافية الشركة وقد يؤدي إلى فرض غرامات قانونية أو فقدان ثقة الأطراف المعنية.

3. خسائر الشركات نتيجة الجرائم الإلكترونية:

الجرائم الإلكترونية تؤدي إلى خسائر مباشرة وغير مباشرة للشركات، منها:

1) الخسائر المالية المباشرة :نتيجة سرقة الأموال من الحسابات البنكية أو دفع فدى إلكترونية.
2) تكاليف استرداد البيانات وإصلاح الأنظمة :حيث تحتاج الشركات إلى استثمارات كبيرة لاستعادة البيانات وتأمين الأنظمة.
3) تعطل الأعمال :الهجمات مثل برمجيات الفدية قد تؤدي إلى توقف العمليات المحاسبية لفترة، مما يؤثر على أداء الشركة.
4) الغرامات التنظيمية :قد تواجه الشركات غرامات إذا تبين أنها لم تلتزم بالإجراءات الأمنية المناسبة لحماية بياناتها.

4. تأثير هذه الجرائم على ثقة المستثمرين:

الجرائم الإلكترونية التي تستهدف البيانات المحاسبية تؤثر بشكل كبير على ثقة المستثمرين في الشركة:

1) انخفاض الثقة المالية :تعرض الشركة للاختراق أو سرقة بياناتها قد يجعل المستثمرين يشكون في قدرتها على إدارة أصولها بأمان.
2) التأثير على سعر الأسهم: يمكن أن تؤدي الجرائم الإلكترونية إلى انخفاض قيمة الأسهم نتيجة لردود فعل سلبية من السوق.
3) سمعة الشركة :الشركات التي تعاني من اختراقات بيانات متكررة تواجه صعوبة في استعادة سمعتها، مما يؤثر على قدرتها على جذب المستثمرين الجدد.

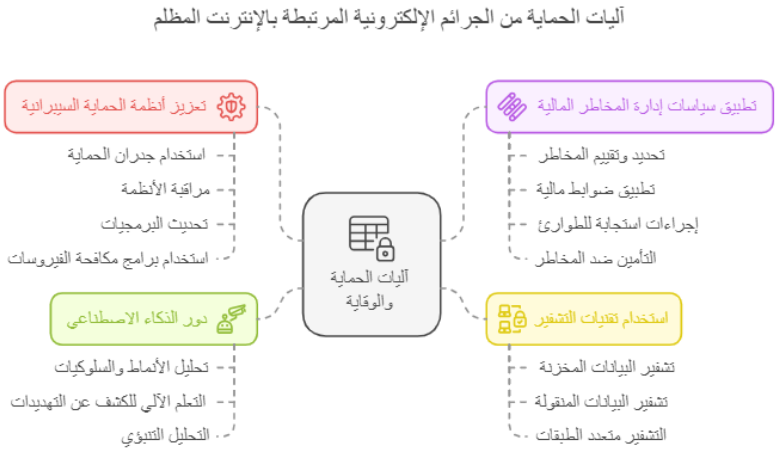
5. آليات الحماية والوقاية من الجرائم الإلكترونية المرتبطة بالإنترنت المظلم:

مجلة صرمان للعلوم والتقنية
Vol7, No.1, Jan-Jun. 2025
Pages: 240 ~ 249

Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)

sjst.scst.edu.ly

آليات الحماية والوقاية من الجرائم الإلكترونية المرتبطة بالإنترنت المظلم يظهره الشكل 3. التالي:



الشكل 3 . يبين اليات الحماية من الجرائم الالكترونية المرتبطة بالأنترنت المظلم

1. تعزيز أنظمة الحماية السيبرانية:

من أجل الوقاية من الجرائم الإلكترونية المرتبطة بالإنترنت المظلم، يجب على الشركات والمؤسسات تعزيز أنظمتها الأمنية السيبرانية [8]. من خلال:

1) استخدام جدران الحماية المتقدمة :تساعد جدران الحماية في منع الوصول غير المصرح به إلى الأنظمة والشبكات.
2) مراقبة الأنظمة بشكل مستمر :يجب مراقبة الشبكات والأنظمة على مدار الساعة للكشف عن أي نشاط غير عادي قد يشير إلى هجوم إلكتروني.
3) تحديث البرمجيات بشكل دوري :تشمل التحديثات تصحيحات الأمان التي تساعد في تقوية الأنظمة ضد الهجمات الإلكترونية الحديثة.
4) استخدام برامج مكافحة الفيروسات والبرمجيات الخبيثة :التي تساعد في اكتشاف وإزالة أي تهديدات قد تؤثر على البيانات المحاسبية أو الأنظمة المالية.

2. تطبيق سياسات إدارة المخاطر المالية:

إدارة المخاطر المالية تعتبر من الآليات الأساسية لحماية البيانات المحاسبية من الهجمات الإلكترونية:

1) تحديد وتقييم المخاطر :يجب على الشركات تحديد المخاطر المحتملة المرتبطة بسرقة البيانات المحاسبية أو التلاعب بها، ومن ثم وضع استراتيجيات للتخفيف منها.
2) تطبيق ضوابط مالية صارمة :مثل فرض صلاحيات محدودة للوصول إلى البيانات المحاسبية وتفعيل آليات الموافقة المزدوجة على المعاملات المالية.
3) إجراءات استجابة للطوارئ :في حال حدوث اختراق أو عملية احتيال مالي، يجب أن تكون الشركات مستعدة للاستجابة الفورية من خلال فرق استجابة للطوارئ تتعامل مع الأزمة بسرعة.
4) التأمين ضد المخاطر :يمكن للشركات التأمين ضد خسائر البيانات أو الهجمات الإلكترونية التي قد تؤثر على العمليات المالية.

3. استخدام تقنيات التشفير:

التشفير هو أحد الحلول الفعالة لحماية البيانات المحاسبية من السرقة أو التلاعب:

1) تشفير البيانات المخزنة :يجب تشفير جميع البيانات المحاسبية الحساسة التي يتم تخزينها على الخوادم لتقليل فرص وصول القراصنة إليها.

2) تشفير البيانات المنقولة :يجب ايضا تشفير البيانات أثناء إرسالها عبر الشبكات لتوفير حماية إضافية ضد التنصت أو التعديل أثناء النقل.
3) التشفير متعدد الطبقات :من خلال استخدام تقنيات مثل التشفير باستخدام مفاتيح طويلة ومعقدة، يمكن جعل البيانات أكثر أمانا في مواجهة أي هجمات.

4. دور الذكاء الاصطناعي في كشف الجرائم الإلكترونية:

الذكاء الاصطناعي (AI) يمكن أن يكون أداة قوية في كشف الجرائم الإلكترونية واتخاذ التدابير الوقائية:

1) تحليل الأنماط والسلوكيات :يستخدم الذكاء الاصطناعي لتحديد الأنماط غير العادية أو السلوكيات الشاذة في الأنظمة المحاسبية أو المالية، مما يساعد في اكتشاف محاولات القرصنة أو التلاعب في وقت مبكر.
2) التعلم الآلي للكشف عن التهديدات :من خلال تقنيات التعلم الآلي، يمكن للأنظمة اكتشاف التهديدات الجديدة والغير معروفة بناءً على البيانات التاريخية، مما يعزز القدرة على مواجهة الهجمات المتطورة.
3) التحليل التنبؤي :يمكن للذكاء الاصطناعي استخدام البيانات المتاحة للتنبؤ بالهجمات المحتملة وتقديم تحذيرات مسبقة للشركات لتفادي الأضرار المحتملة.

باستخدام هذه الآليات الفعالة في حماية البيانات المحاسبية، يمكن تقليل المخاطر الناجمة عن الجرائم الإلكترونية المترابطة مع الإنترنت المظلم وضمان أمان المعلومات المالية وحمايتها من الاستهداف.

6. الأبعاد القانونية والتنظيمية

1. التشريعات المتعلقة بمكافحة الجرائم الإلكترونية:

في ظل تزايد الجرائم الإلكترونية، تم تبني مجموعة من التشريعات على المستوى المحلي والدولي لمكافحة هذه الأنشطة غير القانونية:

1) القوانين الوطنية :في العديد من الدول، تم إنشاء قوانين خاصة بمكافحة الجرائم الإلكترونية، مثل قانون مكافحة جرائم تقنية المعلومات في بعض الدول العربية، التي تهدف إلى حماية الأنظمة الإلكترونية والبيانات المحاسبية من الهجمات الرقمية.
2) قوانين حماية البيانات الشخصية :مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، التي تفرض على الشركات تأمين وحماية بيانات المستخدمين من السرقات أو التلاعب، بما في ذلك البيانات المحاسبية.
3) الحقوق الرقمية والتعويضات :تضمن التشريعات حقوق الأفراد والشركات في حال تعرض بياناتهم للسرقة أو التلاعب، وتتيح لهم اللجوء إلى القضاء للمطالبة بالتعويضات عن الأضرار الناتجة.

2. التعاون الدولي لمواجهة الأنشطة غير القانونية على الإنترنت المظلم:

نظرا للطابع العالمي للإنترنت المظلم، فقد أصبح التعاون بين الدول أمرا بالغ الأهمية لمكافحة الجرائم الإلكترونية:

1) الاتفاقيات الدولية :هناك العديد من الاتفاقيات الدولية التي تهدف إلى تنسيق الجهود بين الدول لمكافحة الجرائم الإلكترونية مثل اتفاقية بودابست لمكافحة الجرائم الإلكترونية التي تم تبنيها من قبل مجلس أوروبا عام 2001، والتي تعتبر أداة قانونية رئيسية في التعاون الدولي.
2) المنظمات الدولية :تعمل منظمات مثل الإنتربول والأمم المتحدة على تنسيق الجهود بين الدول لمكافحة الأنشطة الإجرامية عبر الإنترنت، بما في ذلك على الإنترنت المظلم.
3) التعاون بين الشركات والدول :يتطلب الأمر تعاونا بين الشركات الكبرى والمنظمات الحكومية لتبادل المعلومات بشكل آمن بشأن التهديدات الإلكترونية والاستجابة السريعة للهجمات.

3. العقوبات القانونية المرتبطة بالجرائم الإلكترونية:

تفرض التشريعات العديد من العقوبات القانونية ضد الجرائم الإلكترونية التي تؤثر على البيانات المحاسبية وتختلف هذه العقوبات بناءً على نوع الجريمة وقيمتها:

1) العقوبات المالية :تشمل فرض غرامات مالية ضخمة على الأفراد أو الكيانات القانونية التي تشارك في جرائم سرقة البيانات أو التلاعب المالي.
2) العقوبات السجنية :في بعض الحالات قد يواجه المجرمون السجن لفترات طويلة إذا تم إثبات ارتكابهم لجرائم خطيرة مثل القرصنة الإلكترونية أو الابتزاز الإلكتروني.
3) العقوبات التجارية :يمكن فرض عقوبات على الشركات التي لم تلتزم بالإجراءات الأمنية الكافية لحماية بياناتها من الهجمات الإلكترونية، مثل الغرامات أو إغلاق الأعمال في بعض الحالات.

4) إجراءات قضائية :يمكن للأطراف المتضررة من الجرائم الإلكترونية (مثل الشركات أو الأفراد) تقديم شكاوى قانونية للمطالبة بالتعويضات عن الأضرار التي لحقت بهم نتيجة لاختراق أو سرقة البيانات المحاسبية.

إن تطوير التشريعات والأنظمة القانونية لمواكبة التطورات السريعة في مجال الجرائم الإلكترونية يعد أمرا ضروريا لضمان حماية البيانات المحاسبية والحفاظ على بيئة رقمية آمنة للأفراد والشركات [9].

7. دراسة حالة

دراسات حالة وأمثلة واقعية

1. تحليل أمثلة لشركات تأثرت بجرائم الإنترنت المظلم:

1) **شركة :(2013) "Target"** في عام 2013، تعرضت شركة "Target" لعملية اختراق كبيرة أسفرت عن سرقة بيانات بطاقات ائتمان لأكثر من 40 مليون عميل. الهجوم تم من خلال اختراق أنظمة الشركة عبر الإنترنت المظلم، حيث تمكن القراصنة من الوصول إلى الشبكة الداخلية للشركة واستخدام معلومات العملاء لبيعها على الإنترنت المظلم.

التأثير :

1. **المالي :**تقدر تكاليف هذا الاختراق بحوالي 162 مليون دولار، وذلك بسبب تكاليف التحقيقات والإصلاحات الأمنية والتعويضات للعملاء.
2. **السمعة :**تأثرت سمعة الشركة بشكل كبير، مما أدى إلى فقدان ثقة العملاء وبالتالي انخفاض المبيعات والعائدات في السنوات التالية.

2) **شركة :(2017) "Equifax"** تعرضت شركة Equifax ، التي تعد واحدة من أكبر الشركات المتخصصة في الائتمان والبيانات المالية، لاختراق أدى إلى سرقة بيانات حساسة الى 147 مليون شخص. الهجوم تم باستخدام ثغرة في النظام الأمني وقد تم تداول البيانات المسروقة على الإنترنت المظلم، بما في ذلك أرقام الضمان الاجتماعي وبيانات الحسابات البنكية.

التأثير :

1. **المالي :**تكلفة الحادث تجاوزت 700 مليون دولار بسبب الغرامات القانونية والتحقيقات والإجراءات التعويضية للعملاء.
2. **السمعة :**فقدت الشركة ثقة المستهلكين وأصحاب الأعمال، مما أثر سلبا على العلاقات التجارية المستقبلية والسمعة في السوق المالية.

3) **شركة :(2014) "Sony Pictures"** تعرضت شركة Sony Pictures في عام 2014 لهجوم إلكتروني كبير من قبل مجموعة قرصنة تسمى .Guardians of Peace الهجوم تم باستخدام تقنيات قرصنة عبر الإنترنت المظلم، حيث تم سرقة رسائل بريد إلكتروني وبيانات الموظفين وأفلام غير معلن عنها وتم تسريب هذه الملفات على الإنترنت.

التأثير :

1. **المالي :**خسرت الشركة ملايين الدولارات نتيجة لتسريب الأفلام غير المعلنة وتكاليف التحقيقات والتعويضات.
2. **السمعة :**تأثرت سمعة الشركة بشكل بالغ، حيث تم تسريب معلومات خاصة عن الموظفين والمشاريع المستقبلية، مما أضر بعلاقات الشركة مع الممثلين والمخرجين والجمهور بشكل عام.

2. تأثير الجرائم على سمعة الشركات وأدائها المالي:

التأثير على السمعة:

1. تعرض الشركات لجرائم إلكترونية مرتبطة بالإنترنت المظلم يؤدي إلى فقدان ثقة العملاء والشركاء التجاريين. العملاء يشعرون بالقلق حيال سلامة بياناتهم الشخصية والمالية، مما يؤدي إلى انخفاض الولاء للشركة والابتعاد عنها لصالح منافسين.
2. بالنسبة للمستثمرين، فإن تعرض الشركات لتهديدات أمنية قد يثير القلق بشأن قدرة الشركة على حماية أصولها، مما قد يؤدي إلى تقلبات في سعر الأسهم.

التأثير على الأداء المالي:

1. التكاليف المباشرة :تشمل تكاليف التحقيقات والإصلاحات الأمنية والتعويضات للعملاء المتضررين.
2. الغرامات القانونية :قد تفرض السلطات التنظيمية غرامات كبيرة على الشركات التي لا تتخذ الإجراءات الأمنية الكافية، مما يؤثر على ربحيتها.
3. الخسائر غير المباشرة :تشمل الخسائر المرتبطة بتقليل الثقة في العلامة التجارية وفقدان عملاء وتأثيرات سلبية على العقود التجارية المستقبلية.

4. زيادة في تكاليف التأمين :بعد الهجوم الإلكتروني، قد تواجه الشركات زيادة في تكاليف التأمين ضد الجرائم الإلكترونية، مما يؤثر على الميزانية العامة.

تظهر هذه الأمثلة أن الجرائم الإلكترونية المرتبطة بالإنترنت المظلم ليس فقط تؤثر على الأمان السيبراني للشركات، بل تمتد تأثيراتها بشكل كبير إلى سمعتها وأدائها المالي. لذلك تتطلب الحماية من هذه الجرائم استراتيجيات أمنية قوية ومرنة لضمان استمرارية الأعمال وحماية البيانات المحاسبية والمالية.

8. التوصيات

1. إجراءات لتعزيز أمن البيانات المحاسبية:

1) تطبيق أنظمة أمان متقدمة: من الضروري أن تقوم الشركات بتطبيق أنظمة أمان حديثة ومتطورة مثل جدران الحماية الذكية وبرامج مكافحة الفيروسات المتقدمة وأنظمة الكشف عن التسلل (IDS) لضمان حماية البيانات المحاسبية من أي اختراقات أو هجمات إلكترونية.
2) تشديد إجراءات التحقق من الهوية: يجب تفعيل نظام المصادقة متعددة العوامل (MFA) لجميع الأنظمة التي تحتوي على بيانات محاسبية حساسة لضمان أن الوصول إلى هذه البيانات يتم فقط من قبل الأشخاص المصرح لهم.
3) التشفير الشامل :يجب تشفير جميع البيانات المحاسبية، سواء كانت مخزنة على الخوادم أو أثناء نقلها عبر الشبكات، باستخدام بروتوكولات تشفير قوية مثل AES-256و TLS لضمان عدم تمكن المهاجمين من الوصول إليها.
4) التحديث المستمر للبرمجيات: ضرورة تحديث الأنظمة والبرمجيات بشكل دوري لتصحيح الثغرات الأمنية وتعزيز الحماية ضد التهديدات الحديثة.
5) إجراء اختبارات اختراق دورية: يجب إجراء اختبارات اختراق بشكل منتظم لتحديد نقاط الضعف في الأنظمة والتأكد من قدرتها على التصدي للهجمات الإلكترونية المحتملة.

2. دور المؤسسات في رفع الوعي بالمخاطر الإلكترونية:

1) التدريب المستمر للموظفين: يجب أن تقوم المؤسسات بتوفير برامج تدريبية متكاملة للموظفين حول كيفية التعرف على التهديدات الإلكترونية، مثل الرسائل الاحتيالية (Phishing) والروابط الملوثة والتأكد من اتباع سياسات الأمان الخاصة بالشركة.
2) التثقيف حول سياسات حماية البيانات: يجب على المؤسسات توعية موظفيها بأهمية حماية البيانات المحاسبية والمعلومات الحساسة الأخرى من السرقة أو التلاعب وتوضيح عواقب فشلهم في اتباع سياسات الأمان.
3) إطلاق حملات توعية موجهة للعملاء :يجب أن تقوم الشركات بإطلاق حملات توعية لعملائها حول كيفية حماية بياناتهم الشخصية والمالية، خاصة في ظل الهجمات الإلكترونية المتزايدة التي تستهدف العملاء عبر الإنترنت.
4) إشراك المستشارين الأمنيين: يمكن للمؤسسات التعاقد مع خبراء الأمن السيبراني لإجراء ورش عمل دورية لرفع الوعي حول أفضل ممارسات حماية البيانات من التهديدات.

3. أهمية التعاون بين القطاعين العام والخاص لمكافحة هذه الجرائم:

1) تبادل المعلومات والتنسيق بين الجهات الأمنية: يجب أن يكون هناك تعاون مستمر بين المؤسسات الحكومية والشركات الخاصة لتبادل المعلومات حول الهجمات الإلكترونية وطرق الوقاية منها. يمكن للجهات الحكومية أن توفر مؤشرات تهديد (Threat Indicators) تساعد الشركات على اكتشاف الأنشطة المشبوهة والتعامل معها بشكل أسرع.
2) تطوير تشريعات وسياسات مشتركة: يجب على القطاعين العام والخاص التعاون لتطوير تشريعات وسياسات تحكم عمليات مكافحة الجرائم الإلكترونية. كما يجب تسريع إجراءات تعديل القوانين الحالية لتواكب تطورات الهجمات الإلكترونية الحديثة وتفرض عقوبات رادعة على المجرمين.
3) تعزيز الشراكات بين الحكومات والشركات التكنولوجية: الشركات التكنولوجية الكبرى يجب أن تعمل مع الحكومات لتحسين أدوات الأمن السيبراني وتقديم حلول مبتكرة للوقاية من الجرائم الإلكترونية. يمكن أن تشمل هذه الشراكات تقنيات متقدمة مثل الذكاء الاصطناعي والتحليل التنبؤي للكشف المبكر عن الهجمات.
4) تنظيم تدريبات ومناورات مشتركة: يمكن للقطاعين العام والخاص تنظيم تدريبات جماعية لاختبار جاهزية المؤسسات لمواجهة الهجمات الإلكترونية، مما يساهم في تطوير استراتيجيات استجابة أكثر فعالية في حال وقوع هجوم حقيقي.

إن اتخاذ هذه الإجراءات والتوصيات يمكن أن يسهم بشكل كبير في تعزيز الحماية ضد الجرائم الإلكترونية التي تهدد البيانات المحاسبية ويحد من تأثيراتها السلبية على الشركات والمؤسسات. التعاون المستمر بين القطاعين العام والخاص يشكل عنصراً حيوياً في مواجهة التحديات المتزايدة التي تطرأ في الفضاء الرقمي.

9. الخاتمة

1.9. تلخيص لأهم النقاط والنتائج:

لقد استعرضت هذه الورقة البحثية الأبعاد المختلفة للجرائم الإلكترونية المرتبطة بالإنترنت المظلم وتأثيرها على البيانات المحاسبية. تم توضيح أن الإنترنت المظلم يمثل بيئة خصبة للأنشطة غير القانونية مثل القرصنة وبيع البيانات المحاسبية المسروقة والابتزاز الإلكتروني، مما يشكل تهديدًا حقيقيًا للبيانات المالية الحساسة في الشركات.

1) أثر الجرائم الإلكترونية على البيانات المحاسبية :فقد ثبت أن هذه الجرائم تؤدي إلى سرقة البيانات الحساسة والتلاعب في السجلات المالية وزيادة تكاليف الشركات من حيث التحقيقات والغرامات والتعويضات. كما أن السمعة التجارية والأداء المالي للشركات يتأثر بشكل بالغ نتيجة لهذه الأنشطة الإجرامية.
2) آليات الحماية :تم تحديد العديد من التدابير الوقائية لتعزيز أمان البيانات المحاسبية، مثل استخدام أنظمة أمان متقدمة وتشفير البيانات والمصادقة متعددة العوامل. كما تطرقنا إلى دور الذكاء الاصطناعي في الكشف المبكر عن الجرائم الإلكترونية.
3) الأبعاد القانونية والتنظيمية :تمت مناقشة التشريعات المتعلقة بمكافحة الجرائم الإلكترونية والتعاون الدولي لمكافحة الأنشطة غير القانونية على الإنترنت المظلم. وقد تم تسليط الضوء على العقوبات القانونية المرتبطة بهذه الجرائم وأثرها على الشركات والأفراد.
4) التوصيات :تم اقتراح عدة إجراءات لتعزيز أمن البيانات المحاسبية ورفع الوعي بالمخاطر الإلكترونية من خلال التدريب المستمر للموظفين والتعاون بين القطاعين العام والخاص.

2.9. دعوة لمزيد من البحث في هذا المجال:

إن الجرائم الإلكترونية المرتبطة بالإنترنت المظلم تعتبر تهديدًا متزايدًا يتطلب اهتمامًا أكبر من الأوساط الأكاديمية والصناعية على حد سواء. وعلى الرغم من الجهود المبذولة في هذا المجال، فإن هناك حاجة ملحة لاستمرار البحث في مجالات مثل تطوير تقنيات الأمان وتحسين القوانين المتعلقة بالجرائم الإلكترونية ودراسة تأثيرات هذه الجرائم على الاقتصاد العالمي. كما أن البحث في أساليب الحماية المستدامة والتعامل مع الهجمات المتطورة باستمرار هو أمر حيوي لمواكبة التطورات السريعة في مجال الأمن السيبراني. يجب أن يكون هناك أيضًا تركيز على كيفية تحسين التنسيق بين الحكومات والشركات لمكافحة هذه الجرائم بشكل أكثر فعالية، وبالتالي حماية البيانات المحاسبية من التهديدات الرقمية.

إن تعزيز التعاون بين الباحثين الخبراء في المجال السيبراني والمشرعين سيسهم في خلق بيئة رقمية أكثر أمانًا، مما يعود بالنفع على الشركات، العملاء، والمجتمع ككل.

10. المراجع

[1]. Hurlburt, George. "Shining light on the dark web." *Computer* 50.04 (2017): 100-105.
[2] .Dumitrașcu, D .(2020) .Understanding the Dark Web: An Overview of the Hidden Part of the Internet .Journal of Cybersecurity and Privacy, 6(4), 145-162 .
[3]. Rahman, Md Rayhanur, Rezvan Mahdavi Hezaveh, and Laurie Williams. "What are the attackers doing now? Automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey." *ACM Computing Surveys* 55.12 (2023): 1-36.
[4]. Saleem, Javeriah, Rafiqul Islam, and Muhammad Ashad Kabir. "The anonymity of the dark web: A survey." *Ieee Access* 10 (2022): 33628-33660.
[5]. Chen, Hsinchun. "Dark web: Exploring and mining the dark side of the web." *2011 European Intelligence and Security Informatics Conference*. IEEE, 2011.
[6]. Rawat, Romil, et al. "Cognitive systems for dark web cyber delinquent association malignant data crawling: A review." *Handbook of Research on War Policies, Strategies, and Cyber Wars* (2023): 45-63.
[7]. Kaur, Shubhdeep, and Sukhchandan Randhawa. "Dark web: A web of crimes." *Wireless Personal Communications* 112 (2020): 2131-2158.
[8]. Coburn, Andrew, Eireann Leverett, and Gordon Woo. *Solving cyber risk: protecting your company and society*. John Wiley & Sons, 2018.
[9]. De Goede, Marieke. "The SWIFT affair and the global politics of European security." *JCMS: Journal of Common Market Studies* 50.2 (2012): 214-230.

Surman Journal for Science and Technology
ISSN: Online (2790-5721) - Print (2790-5713)
مجلة صرمان للعلوم والتقنية
Vol**7**, No.**1**, Jan-Jun. 2025
Pages: 240 ~ 249