جامعة غرداية

كلية العلوم الاقتصادية و التجارية وعلوم التسيير

قسم علوم التسيير

بالتعاون مع مخبر الدراسات التطبيقية في العلوم المالية والمحاسبة

ينظمون ملتقى وطني (حضوري/ عن بعد) بعنوان:

" مخاطر الهندسة الاجتماعية ومتطلبات تحقيق الأمن المجتمعي للمؤسسات الاقتصادية"، يوم 04 ماي 2025.

مداخلة بعنوان:

دور البيانات في الاقتصاد الرقمي وتكاليف الهندسة الاجتماعية نظرة للواقع وطرق الاستجابة للتغيرات

إعداد الباحث :

- مصيطفى عبد اللطيف، أستاذ ، جامعة غرداية، messaitfa.abdellatif@univ-ghardaia.edu.dz

من خلال المحور رقم: 1

الملخص: (لا يتجاوز 150 كلمة)

يشهد العالم الرقمي تسارعا و تحولاًت جذريةً في بنية الاقتصاد العالمي، حيث أصبحت **البيانات الضخمة (Big Data)** أحد أهم الأصول الاستراتيجية والمحرك الاساسي للنمو والابتكار في مختلف القطاعات. تُسهم هذه البيانات في تحسين كفاءة الأسواق والمؤسسات ، وتطوير المنتجات وتقديم خدمات مبتكرة، وتعزيز صنع القرار في القطاعات الاقتصادية المختلفة. ومع ذلك، فإن هذا التوسع في استخدام البيانات يطرح تحديات ومخاطر كبيرة، أبرزها **تكاليف الهندسة الاجتماعية** الناتجة عن استغلال الثغرات الأمنية أو التلاعب السلوكي، مما يؤثر على الثقة في المنظومة الرقمية ويُهدد استقرار الاقتصاد القائم على البيانات.

يهدف هذا البحث إلى استكشاف **دور البيانات الضخمة في دفع عجلة الاقتصاد الرقمي**، مع تحليل التكاليف الخفية المرتبطة بالهندسة الاجتماعية، وتأثيراتها السلبية على المؤسسات والاسواق والاقتصاديات.

يسعى هذا البحث إلى تقديم نظرة حول الواقع ورؤية لكيفية الاستجابة للتحديات التي تفرضها الهندسة الاجتماعية .

كلمات مفتاحية: بيانات ضخمة، هندسة اجتماعية، اقتصاد رقمي، هجمات سيبرانية .

Abstract:

The digital world is witnessing rapid and radical transformations in the structure of the global economy, where **Big Data** has emerged as one of the most critical strategic assets and a primary driver of growth and innovation across sectors. This data enhances market and institutional efficiency, enables product development and innovative services, and supports decision-making in various economic domains. However, the expanding use of data poses significant challenges and risks, most notably the costs of **social engineering**—such as exploiting security vulnerabilities or behavioral manipulation—which undermine trust in digital systems and threaten the stability of data-driven economies.

This research explores the role of Big Data in advancing the digital economy while analyzing the hidden costs associated with social engineering and its adverse effects on institutions, markets, and economies. By examining current realities, the study aims to provide insights and a forward-looking perspective on addressing the challenges posed by social engineering.

Keywords: Big data, social engineering, digital economy, cyber attacks.

1. مقدمة:

يشهد العالم الرقمي تسارعا وتحولاًت جذريةً في بنية الاقتصاد العالمي، حيث أصبحت **البيانات الضخمة (Big Data)** أحد أهم الأصول الاستراتيجية والمحرك الاساسي للنمو والابتكار في مختلف القطاعات. تُسهم هذه البيانات في تحسين كفاءة الأسواق والمؤسسات ، وتطوير المنتجات وتقديم خدمات مبتكرة، وتعزيز صنع القرار في القطاعات الاقتصادية المختلفة. ومع ذلك، فإن هذا التوسع في استخدام البيانات يطرح تحديات ومخاطر كبيرة، أبرزها **تكاليف الهندسة الاجتماعية** الناتجة عن استغلال الثغرات الأمنية أو التلاعب السلوكي، مما يؤثر على الثقة في المنظومة الرقمية ويُهدد استقرار الاقتصاد القائم على البيانات.

إن التدفق الهائل والمتنوع للبيانات، يُمثل كنزاً أكثر قيمة من الموارد التقليدية كالنفط، فقد أصبحت العملة الصعبة والوقود الجديد في الاقتصاد العالمي. وأصبحت القدرة على جمع وتخزين ومعالجة وتحليل هذه الكميات الهائلة من البيانات بسرعة وكفاءة مصدر الشركات لتحقيق ميزة تنافسية مستدامة وتحقيق عوائد غير عادية.

تعمل البيانات الضخمة وتحليلاتها وتطبيقاتها كحجر الزاوية في التحليل الاقتصادي، وكمؤشرات لقدرة المنظمات على الابتكار للاستجابة لفرص السوق واتخاذ القرارات الملائمة وتحقيق الاستقرار الاقتصادي وتحسين جودة الحياة .

ومع ذلك، فإن التطورات التكنولوجية المتسارعة وازدياد الاعتماد على البيانات الرقمية في شتى مجالات الحياة، المالية والصحية واللوجستية فتح الباب واسعاً أمام تحديات وتهديدات ومخاطر جديدة، تتطلب مراجعة دقيقة واستثمار شامل في الاقتصاد الرقمي ومخاطره واستجابة فعالة للمخاطر المحيطة بالاقتصاديات الرقمية.

ومن بين هذه المخاطر، التي تبرز بقوة في الوقت الحالي والتي اخذت تتعاظم تهديداتها وتتزايد تكاليفها على المؤسسات والدول تبرز تهديدات الهندسة الاجتماعية (Social Engineering) كأحد أبرز التهديدات والتحديات الأمنية التي تواجه الأفراد والمؤسسات والدول على حد سواء.

فالهندسة الاجتماعية القائمة على استغلال الجوانب النفسية والسلوكية واستغلال أحدث التطورات كالذكاء الاصطناعي تستهدف العنصر البشري بدلًا من الأنظمة التقنية وتتلاعب بهم لكسب ثقتهم فتخترق حواجز الثقة للوصول إلى المعلومات السرية، وأصبحت تشكل تهديداً حقيقياً لأمن المعلومات وسلامة الأنظمة الرقمية واستراتيجيات الدول، مما يؤدي إلى خسائر مالية فادحة وتشويه السمعة وتعطيل للعمليات الاقتصادية .

يسعى هذا البحث إلى ابراز كيف تُساهم البيانات الضخمة في تشكيل ملامح الاقتصاد الرقمي وكيف تؤثر على الاقتصاد، وفي الوقت ذاته تتعرض البيئة الرقمية المتزايدة لخطر متزايد من هجمات الهندسة الاجتماعية والتي لها تأثيرات اقتصادية واجتماعية بالغة ومكلفة.

يهدف هذا البحث إلى استكشاف دور البيانات الضخمة في دفع عجلة الاقتصاد الرقمي، مع تحليل التكاليف الخفية المرتبطة بالهندسة الاجتماعية، وتأثيراتها السلبية على المؤسسات والاسواق والاقتصاديات.

يسعى هذا البحث إلى تقديم نظرة حول الواقع ورؤية لكيفية الاستجابة للتحديات التي تفرضها الهندسة الاجتماعية .

بالإضافة إلى ذلك، سنسعى إلى اقتراح إطار عمل شامل يتضمن استراتيجيات وتدابير وقائية فعالة يمكن للمؤسسات والأفراد والدول تبنيها لتعزيز الأمن الرقمي والتخفيف من مخاطر الهندسة الاجتماعية في عصر البيانات الضخمة.

تعريف اقتصاد البيانات BIG DATA

يعرف بأنه «القيمة المالية والاقتصادية التي ينتجها تخزين كميات ضخمة من البيانات التجارية والحكومية وتحليلها واسترجاعها بسرعة كبيرة عبر برمجيات معقدة وأدوات أخرى (مؤسسة دبي للمستقبل، ماي 2021، تقرير اقتصاد البيانات الجديد، ص: 8)

أهمية البيانات

- البيانات العملة الصعبة في الاقتصاد العالمي,
- وقود الاقتصاد الجديد
- له قيمة اقتصادية كبيرة في الاقتصاد الرقمي
- البيانات هي حجر الزاوية في التحليل الاقتصادي، فبدون بيانات دقيقة وموثوقة ، لا يمكن للاقتصاديين تقديم تنبؤات أو توصيات ذات مغزى.
- تحسين اتخاذ القرارات,
- الاستقرار الاقتصادي,
- محفزًا للنمو الاقتصادي والابتكار,
- تحسين جودة الحياة

تعريف البيانات الضخمة:

تعرف المنظمة الدولية للمعايير ISO البيانات الضخمة بأنها مجموعة أو مجموعات من البيانات لها خصائصها الفريدة مثل الحجم، السرعة، التنوع، التباين، صحة البيانات,

كما يعرفها الاتحاد الدولي للاصالات ITU تشير الى مجموعات البيانات التي تتميز بأنها فائقة الحجم والسرعة والتنوع,وقد أصبح التقنيون يعتمدون على أنظمة الذكاء الاصطناعي وتقنيات الحوسبة السحابية

- هي البيانات التي تقاس بالبيتابايت petabyte) ألف تيرا بايت(أو الايكسابايت exabyte) مليون تيرا بايت(, أو الزيتابايت Zettabytes) مليار تيرا بايت(

عرفها قاموس جارتنر بأنها" أصول معلوماتية كبيرة الحجم وعالية السرعة و / أو عالية التنوع تتطلب أشكالا مبتكرة وفعالة من حيث التكلفة لمعالجة المعلومات التي تتيح تحسين الرؤية واتخاذ القرار "data,) https://www.gartner.com/en/information-technology/glossary/big- 2015

من خصائصها : القيمة، الدقة، السرعة، التنوع والحجم

الشركات الرائدة في اقتصاد البيانات[1] :

شركات التكنولوجيا العملاقة : جوجل، أمازون، مايكروسوفت، فيسبوك، أبل.(GAFAM)

شركات تحليل البيانات: Palantir، Snowflake، Tableau، SAS،.Splunk

مزودو خدمات السحابة: AWS، Microsoft Azure، Google Cloud، .IBM Cloud

الشركات الناشئة المتخصصة: شركات متخصصة في الذكاء الاصطناعي وتعلم الآلة.

حجم اقتصاد البيانات العالمي:

الرقمي التحول نسبة المؤسسات في الكبرى العالمية	البيانات متوقع حجم 2026	السوقية القيمة البيانات لاقتصاد 2023 في	الأمم المتحدة: اقتصاد البيانات العالمي بحلول 2030	تمثل البيانات من الناتج المحلي الإجمالي في الاقتصادات المتقدمة	الوظائف التي خلقها اقتصاد البيانات	استثمارات البيانات:
87%	زيتابايت 552	تريليون $3	13 تريليون دولار حجم	نحو 10%-7%	ألمانيا (1.95مليون) المملكة المتحدة (1.65مليون) هولندا)349,000(	تظهر الدراسات أن كل دولار مستثمر في أنظمة البيانات يمكن أن يولد ما بين 7 إلى 73 دولار من الفوائد الاقتصادية، بمتوسط 32 دولار

1 زيتابايت يعادل 1 مليارتيرابايت

source : data4sdgs.org, New analysis shows every dollar invested in data systems creates ...Data is a secret weapon, making overseas aid and domestic spending more impactful.

نماذج الأعمال بقيادة البيانـــــات

[1] أنظر:

- أهم الشركات الناشئة في مجال البيانات الضخمة التي يجب متابعتها في عام 2021، https://fastercapital.com/arabpreneur/
- 35 Top Data Science Companies You Should Know in 2025, https://innovatureinc.com/top-10-big-data-companies/
- Top 10 Big Data Companies to Know in 2025, https://innovatureinc.com/top-10-big-data-companies/

تنتج الشركات الرقمية منافع جديدة من البيانات الملتقطة لحظيا من منصاتها، والواقع أن حصة كبيرة من النمو والنجاح الذي حققته الشركات العملاقة في قطاع التقنية، مثل أمازون وفيسبوك وجوجل ونتفلكس، يعود إلى كمية البيانات التي تجمعها وتستخدمها.

تكنولوجيات تمكين اقتصاد البيانات:

- الحوسبة السحابية: بنية تحتية مرنة وقابلة للتوسع لتخزين ومعالجة كميات ضخمة من البيانات [2].
- الذكاء الاصطناعي: خوارزميات متقدمة لاستخراج الرؤى واتخاذ القرارات التلقائية من البيانات[3].
- إنترنت الأشياء: أجهزة متصلة تجمع بيانات من العالم المادي وترسلها للتحليل.
- تقنية البلوكتشين: سجلات لامركزية لتبادل البيانات بطريقة آمنة وشفافة بين الأطراف.

مفهوم أمن البيانات[4]:

أمن البيانات هو ممارسة حماية المعلومات الرقمية من الوصول غير المصرح به أو التلف أو الضياع. يتضمن تنفيذ التقنيات والأدوات والسياسات لضمان بقاء البيانات آمنة طوال دورة حياتها.
يتضمن أمان البيانات طرقا مثل التشفير والتحكم في الوصول والتدقيق المنتظم لمنع الانتهاكات وضمان الامتثال للوائح.

هو ممارسة حماية البيانات الرقمية من الوصول أو الاستخدام أو الإفصاح غير المصرح به بطريقة تتفق مع استراتيجية المخاطر الخاصة بالمؤسسة. ويشمل أيضا حماية البيانات من التعطيل أو التعديل أو التلف[5].

يشير أمن البيانات إلى مجموعة التقنيات والأدوات والضوابط والعمليات والإجراءات المصممة لضمان سرية البيانات وسلامتها وتوافرها[6]

---

[2] توركان أحمد خليل، ألماس احمد خليل، الحوسبة السحابية الواقع والتحديات، المؤتمر العلمي الدولي الاول لنقابة الاكاديميين العراقيين/ مركز التطور الاستراتيجي الاكاديمي تحت عنوان "العلوم الانسانية والصرفة رؤية نحو التربية والتعليم المعاصرة، 11-12شباط 2019م ، جامعة دهوك – العراق، ص: 5

[3] بسمة عمر الخطاب، تطبيقات الذكاء الاصطناعي، المجلة العلمية للملكية الفكرية وادارة الابتكار، جامعة حلوان، مصر، ص ص: 258 - 260.

[4] What Is Data Security? Data Security Definition + Overview, https://www.sailpoint.com/identity-library/.

[5] What is Data Security?Narendran Vaideeswaran - September 18, 2023, https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/data-security/ ,

[6] Guide to Data Security and Privacy, Guihttps://www.sailpoint.com/identity-library/data-security-privacyde to Data Security and Privacy

ومن الجدير بالذكر وجود مفهوم اقتصادي جديد أُطلق عليه مصطلح "ناتج البيانات الإجمالي" تماشياً مع مصطلح "الناتج المحلي الإجمالي" لتحديد أكبر منتجي "البيانات الإجمالية" في العالم، وذلك باستخدام أربعة معايير: حجم البيانات، ومعدلات الاستخدام، وإمكانية الوصول للبيانات، ودرجة التعقيد في تحليلها والاستفادة منها.

التحول الرقمي والمخاطر المصاحبة:

ترى منظمة التعاون والتنمية الاقتصادية أن التحول الرقمي عملية تتضمن كثيرا من التقنيات الرقمية كتقنية الجيل الخامس، والذكاء الاصطناعي والبيانات الضخمة وتقنية سلسلة الكتل، بحيث تشكل هاته التقنيات نظاما بيئيا تنشأ من خلاله تغيرات اقتصادية واجتماعية في المستقبل [7]

تسارع التحول الرقمي: شهد العالم خلال السنوات الأخيرة تسارعاً غير مسبوق في عمليات التحول الرقمي، حيث أصبحت البيانات العمود الفقري للاقتصادات الحديثة والشركات العالمية. هذه النقلة النوعية أتاحت فرصاً استثنائية للنمو والابتكار.

زيادة سطح الهجوم: مع تزايد الاعتماد على التقنيات الرقمية، اتسعت مساحة التعرض للهجمات السيبرانية بشكل كبير. أصبحت البنية التحتية الرقمية هدفاً مغرياً للقراصنة والجهات الخبيثة الساعية لتحقيق مكاسب مالية أو استراتيجية.

تعقيد المشهد الأمني: تطورت تقنيات الهجوم بشكل ملحوظ، مما جعل المشهد الأمني أكثر تعقيداً وصعوبة. لم تعد التهديدات تقتصر على المتسللين الأفراد، بل امتدت لتشمل مجموعات الجريمة المنظمة والجهات المدعومة من دول، مما زاد من خطورة وتأثير الهجمات.

مزايا الاقتصاد الرقمي[8] : يوفر الاقتصاد الرقمي العديد من الفوائد ، والتي ساهمت في توسعه السريع وتأثيره الإيجابي على مجموعة متنوعة من الصناعات:

- **زيادة الإنتاجية.** يمكن للشركات تحسين إنتاجيتها وكفاءتها باستخدام التكنولوجيا الرقمية لأتمتة عملياتها وعملياتها.
- **انخفاض التكاليف.** تلغي الحوسبة السحابية والأطر الرقمية الحاجة إلى بنية تحتية مادية كبيرة ونفقات رأسمالية ، مما يمكن المؤسسات من التوسع والتقليل حسب الحاجة.
- يمكن للشركات من تعزيز الاقتصاد العالمي والتواجد من خلال المنصات والتقنيات عبر الإنترنت .
- **الوصول إلى المزيد من البيانات.**

[7] OECD (2019). "Digital transformation and capabilities ", in Supporting Entrepreneurship and Innovation in Higher Education in Italy. OECD Publishing,Paris. P : 73.

[8] DATA AS ECONOMIC GOODS: DEFINITIONS, PROPERTIES, CHALLENGES, ENABLING TECHNOLOGIES FOR FUTURE DATA MARKETS Yuri Demchenko, Wouter Los, Cees de Laat System and Networking Lab, University of AmsterdamITU Journal: ICT Discoveries, Special Issue No. 2, 23 Nov. 2018

- **التخصيص وتحسين تجربة العملاء: .** باستخدام تحليلات البيانات الذكاء الاصطناعي ، يمكن للشركات تخصيص المنتجات والخدمات والحملات التسويقية ، مما يؤدي في النهاية إلى تحسين رضا العملاء.

عيوب الاقتصاد الرقمي: في حين أن الاقتصاد الرقمي يوفر العديد من المزايا ، إلا أنه يمثل أيضا التحديات التالية:

- **مخاوف تتعلق بالخصوصية والأمان.** يعتمد الاقتصاد الرقمي بشكل كبير على الحصول على البيانات الشخصية وتخزينها ، مما قد يخلق مشكلات تتعلق بخصوصية البيانات وأمنها. يمكن أن تؤدي أحداث مثل خروقات البيانات والهجمات الإلكترونية والوصول غير المصرح به إلى السجلات الخاصة إلى خسائر مالية وسرقة الهوية ونتائج سلبية مختلفة.
- **موجات من الاضطراب.** أنشأ الاقتصاد الرقمي شركات جديدة وطرقا جديدة للتفاعل. ومع ذلك ، واجهت العديد من الشركات والصناعات التي لم تستطع أو لم تستطع الاستفادة من التقنيات لتغيير عملياتها انخفاضا في المبيعات وانخفاض حصتها في السوق وحتى الانهيار الكامل. على سبيل المثال ، أغلقت Blockbuster ومتاجر تأجير المحتوى الأخرى التي لم تتبنى تقنيات البث بسرعة كافية عملياتها. تعد صناعة سيارات الأجرة أيضا مثالا آخر ، حيث تكافح للتنافس على العملاء الذين يجدون Uber و Lyft أسهل في الاستخدام.
- **النزوح الوظيفي.** يمكن أن تحل الأتمتة والرقمنة محل الوظائف ، مما يجعل بعض الأدوار قديمة. قد يحتاج الأفراد إلى اكتساب مهارات جديدة من أجل التوظيف المستمر ، مما قد يتسبب في بطالة مؤقتة واضطراب اقتصادي.
- **احتكار.** أدت رقمنة الاقتصاد إلى اكتساب عدد صغير من مقدمي الخدمات الكبار مثل Apple و Amazon و Google قوة كبيرة ، مما أدى إلى ظروف احتكارية في قطاعات معينة.
- **الفجوة الرقمية.** إن وجود فجوة رقمية ، والتي تشير إلى التفاوت بين أولئك الذين لديهم إمكانية الوصول إلى التكنولوجيا وأولئك الذين لا يملكون ، هو عيب بارز في الاقتصاد الرقمي. ويمكن أن يؤدي هذا الانقسام إلى عدم المساواة فيما يتعلق بالحصول على المعلومات والتعليم وفرص العمل والتقدم الاقتصادي.
- **البصمة البيئية.** إن استخدام الطاقة في الاقتصاد الرقمي في مراكز البيانات وإنتاج الأجهزة الإلكترونية له عواقب بيئية ، مع زيادة الطلب على الخدمات الرقمية مما يؤدي إلى زيادة انبعاثات الكربون والنفايات الإلكترونية والبصمة البيئية الأكبر.

ما هي الهندسة الاجتماعية؟

إنها اسلوب للخداع يتبعه المتصيدون لاغراء الضحايا للافصاح عن بياناتهم الشخصية الحساسة أو القيام باجراءات من شانها ان يحصلوا على اموالهم او معلومات قيمة او سرية، يعتمد المتصيد على أساليب نفسية اجتماعية لخداع ضحيته، كانتحال صفة رجال السلطة العامة او استدراج الضحية بالاغراء[9]

أنواع هجمات الهندسة الاجتماعية:

التصيد الاحتيالي: رسائل احتيالية تبدو شرعية لسرقة البيانات.

انتحال الشخصية: تقمص شخصيات موثوقة للتلاعب بالضحايا.

التصيد الصوتي: مكالمات هاتفية مخادعة للحصول على معلومات حساسة.

التصيد عبر الرسائل: رسائل نصية تحتوي على روابط ضارة.

هجما ت الهندسة الاجتماعية

تتزايد هجمات الهندسة الاجتماعية بسرعة في شبكات اليوم، مما يُضعف سلسلة الأمن السيبراني. وتهدف هذه الهجمات إلى التلاع بالأفراد والشركات لإفشائها بيانات قّيمة وحساسة لصالح مجرمي الإنترنت .

تشكل الهندسة الاجتماعية تحديًا لأمن جميع الشبكات بغض النظر عن مدى قوة جدران الحماية، وأساليب التشفير، وأنظمة كشف التسلل، وبرامج مكافحة الفيروسات، حيث يميل البشر إلى الثقة بالآخرين أكثر من الحواسيب أو التقنيات الأخرى، لذلك فهم الحلقة الأضعف في سلسلة الأمن.

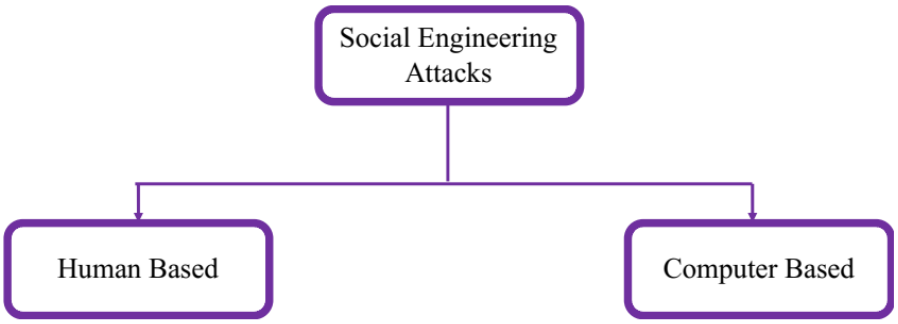
تؤثر الأنشطة الخبيثة التي تتم من خلال التفاعلات البشرية على الشخص نفسيا، مما يدفعه إلى الكشف عن معلوما تسرية أو كسر إجراءات الأمن ونتيجة لهذه التفاعلات البشرية، تُعتبر هجمات الهندسة الاجتماعية أقوى الهجمات لأنها تُهدد جميع الأنظمة والشبكات

على سبيل المثال، تعرضت شركة إيكويفاكس Equifax للاختراق لعدة أشهر وسرقت بيانات حساسة لعملائها ف ي عام 2018 هذه الشركة هي وكالة لإعداد تقارير ورصد ائتمان المستهلكين، تجمع بيانات الأفراد والمستهلكين من الشركات لمراقبة تاريخهم الائتمان ي ومنع عمليات الاحتيال ونتيجة لهذه السرقة للبيانات، تمكن المهاجمون من الوصول إلى المعلومات الشخصية لـ 145.5مليون مستهلك أمريكي. تم سرقة العناوين وأرقام الهواتف والضمان الاجتماعي واختراق بطاقات الائتمان جاء هذا الاختراق نتيجةً لهجمات تصيد احتيالي نُفذت بإرسال آلاف رسائل البريد الإلكتروني متظاهرةً بأنها من مؤسسات مالية أو بنوك كبيرة مثل بنك أوف أمريكا. لا يزال مستخدمو Equifax قلقين بشأن هذا الاختراق الذي شنّه مهاجمون إلكترونيون[10]

تصنيف هجمات الهندسة الاجتماعية: يمكن تصنيف هجما ت الهندسة الاجتماعية إلى فئتين: هجما ت تعتمد على الإنسان أو هجمات تعتمد على الكمبيوتر كما هو موضح في الشكل

[9] حسام نبيل الشنراقي، التصيد الاحتيالي في ظل التطور التقني" انماطه – تحديات المكافحة – الحلول " "دراسة تحليلية"، مجلة الدراسات القانونية والاقتصادية، دورية علمية محكمة - المجلد العاشر العدد الثالث "سبتمبر 2024، ص ص: 2421-2422 .

[10] Social Engineering Attacks: A Survey Fatima Salahdine * and Naima Kaabouch, p 2- 4



إحصاءات مقلقة:

85 %من الاختراقات تتضمن عنصر الهندسة الاجتماعية.

17,8 $ B خسائر سنوية بسبب هجمات الهندسة الاجتماعية عالميًا.

43 %من الموظفين لا يتلقون تدريبًا كافيًا للتعرف على الهجمات.

البيان	معدل النمو السنوي المركب لعدد الهجمات السيبرانية	متوسط تكلفة اختراق البيانات للشركة الواحدة في عام 2022	متوسط التكلفة	الخسائر المتوقعة عالمياً بسبب الجرائم السيبرانية بحلول عام 2025
القيمة	69%	7%	$4.35M	$8.44T

الإحصائيات العالمية للاختراق 2023-2024

البيان	متوسط تكلفة الاختراق	متوسط عدد الأيام للكشف عن الاختراق واحتوائه	نسبة المؤسسات التي تعرضت لأكثر من اختراق	نسبة الارتفاع في هجمات البرامج
القيم	$4.35M ارتفاع بنسبة 15% عن العام السابق	277	83%	60%

المشهد الحالي للتهديدات السيبرانية

هجمات التصيد والهندسة الاجتماعية: تشكل 33 % من اختراقات البيانات، وتزداد تعقيداً مع توظيف الذكاء الاصطناعي. يمكن أن يؤدي هجوم تصيد ناجح إلى خسائر تتراوح بين 500 ألف و4 مليون دولار للشركة الواحدة.

توزيع التكلفة العالمية للجرائم السيبرانية حسب المنطقة

تتباين تكلفة الجرائم السيبرانية بشكل كبير عبر المناطق الجغرافية، مع تركز النصيب الأكبر في المناطق الأكثر تقدماً رقمياً. تتحمل أمريكا الشمالية وأوروبا معاً أكثر من 66 %من التكلفة العالمية، ويرجع ذلك جزئياً إلى ارتفاع مستوى التحول الرقمي وقيمة البيانات المستهدفة في هذه المناطق.

على الرغم من النسبة المنخفضة نسبياً في الشرق الأوسط وأفريقيا، إلا أن معدل نمو التكلفة في هذه المناطق هو الأعلى عالمياً، بزيادة سنوية تتجاوز 15%، مدفوعة بالتوسع السريع في مبادرات التحول الرقمي مع ضعف في البنية التحتية الأمنية.

الدول الأكثر تضرراً من الهجمات السيبرانية

ألمانيا والمملكة المتحدة: تتكبد ألمانيا خسائر سنوية تقدر بـ 0.62 تريليون دولار، بينما تصل خسائر المملكة المتحدة إلى 0.59 تريليون دولار .تمثل هذه الخسائر حوالي 5.7%و6.4 % من الناتج المحلي الإجمالي لكل منهما على التوالي.

الصين: تأتي الصين في المرتبة الثانية عالمياً، مع خسائر تقدر بـ 0.92 تريليون دولار سنوياً. تمثل هذه الخسائر حوالي 6.3 % من ناتجها المحلي الإجمالي.

الولايات المتحدة: تتحمل الولايات المتحدة النصيب الأكبر من تكلفة الهجمات السيبرانية عالمياً، بحوالي 1.79 تريليون دولار سنوياً. تمثل هذه التكلفة حوالي 7.6% من الناتج المحلي الإجمالي الأمريكي.

تأثير الهجمات السيبرانية على نمو الناتج المحلي الإجمالي العالمي

تؤثر الهجمات السيبرانية بشكل سلبي على معدلات النمو الاقتصادي العالمي من خلال تقويض ثقة المستثمرين وتعطيل الأعمال وتشتيت الموارد. وفقاً لتقديرات البنك الدولي، يمكن أن تؤدي الزيادة في وتيرة وحجم الهجمات السيبرانية إلى تباطؤ النمو العالمي بنسبة تصل إلى 4.2% سنوياً.

تشير دراسات اقتصادية إلى أن المخاوف المتعلقة بالأمن السيبراني تؤدي إلى انخفاض الاستثمارات في مشاريع التحول الرقمي بنسبة تتراوح بين 18% و26%، مما يحد من إمكانات النمو الاقتصادي المستقبلي.

2.1.اقتصاديا ت الأمن السيبراني

لقد غذت تكنولوجيا المعلومات النمو الاقتصادي على مدى العقود الثلاثة الماضية عبر الصناعات والشركات ،والأفراد في حين ساهمت تكنولوجيا المعلومات في تعزيز التكامل العالمي، وزيادة الابتكار على مستوى الشركات، وزيادة تنوع المنتجات ، وانخفاض تكاليف أداء المهام الروتينية ,

خروقات البيانات ونتائج الشركات : عرّف خرق البيانات بأنه "نقل أو إفصاح غير مصرح بها لمعلومات حساسة إلى جهة، عادًة ما تكون خارج المؤسسة، غير مخولة بالاطلاع على المعلومات [11]

هناك عدد لا يحصى من الأسباب التي تدعو إلى الحذر من التكرار المتزايد لانتهاكات البيانات. حيث قّدر معهد بونيمون، و هو مركز أبحا ث مستقل يُجري تحليلات سنوية لاختراقات البيانات، أن متوسط عدد حالا ت الاختراق الناجحة لكل شركة بلغ 130حالة في عام 2017 ويمثل هذا زيادة بنسبة 27%عن عام 2016 مما يُترجم إلى تكلفة متوسطة قدر ها 11.7مليون دولار أمريكي لكل مؤسسة لهجمات الجرائم الإلكترونية. 31وبالنسبة للمستهلكين، يزيد هذا حتًما من احتمالية سرقة الهوية والاحتيال في حال كشف معلوماتهم الشخصية في هذه الاختراقات. ووفقا لإحدى الدراسات، وقع 16.7مليون مستهلك أمريكي ضحية لاحتيال الهوية في عام ،2017 مما أدى إلى سرقة ما يقارب 16.8مليار دولار أمريكي[12] .

نقاط الضعف البشرية المستغلة

- **الخوف:** استغلال مخاوف الناس من العقوبات أو المشاكل المالية، التحذير من إغلاق الحسابات.
- **الطمع:** إغراء الأفراد بعروض مالية تبدو مغرية ومربحة، فرص استثمار خيالية.
- **الفضول:** استغلال فضول الإنسان الطبيعي لاكتشاف المجهول.

تكلفة عدم الاستثمار في الأمن السيبراني:

تشير الدراسات إلى أن الشركات التي تستثمر أقل من 3% من ميزانية تكنولوجيا المعلومات في الأمن السيبراني تواجه خطر خسائر تزيد بنسبة 76% عن الشركات التي تخصص 10% أو أكثر. يعد هذا الاستثمار المنخفض مشكلة خاصة في الشركات الصغيرة والمتوسطة، حيث تفتقر 62% منها إلى الموارد اللازمة للتعافي من هجوم سيبراني كبير.

يقدر الخبراء أن كل دولار يتم استثماره في الأمن السيبراني يوفر ما بين 2.5 إلى 3.7 دولار في تكاليف الحوادث المحتملة، مما يجعله من أكثر الاستثمارات فعالية من حيث التكلفة لحماية قيمة الأعمال.

ما هي سرقة البيانات؟

حادث أمني يتم فيه الوصول غير المصرح به أو سرقة معلومات حساسة من نظام أو شبكة، معلومات شخصية، بيانات مالية، ملكية فكرية، معلومات العملاء، أسرار تجارية،

التكلفة غير المباشرة لاختراق البيانات

تضرر السمعة والثقة: تشير الدراسات إلى أن 65% من العملاء يفقدون الثقة في الشركات التي تتعرض لاختراق بياناتهم، وقد يستغرق استعادة هذه الثقة سنوات. يمكن أن تنخفض قيمة العلامة التجارية بنسبة تصل إلى 31% بعد حوادث كبرى.

---

[11] *Ping Wang, ،Hubert D'Cruze ،David Wood* ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES, p162

[12] *THE DATA BREACH DILEMMA: PROACTIVE SOLUTIONS FOR PROTECTING CONSUMERS' PERSONAL INFORMATION DANIEL J. MARCUS† p: 557,*

انخفاض قيمة الأسهم: تنخفض قيمة أسهم الشركات المتضررة بمتوسط 7.27% بعد الإعلان عن اختراق البيانات، وقد تستغرق 46 يوماً في المتوسط للتعافي. بعض الشركات الكبرى شهدت خسائر تجاوزت المليارات في قيمتها السوقية.

فقدان العملاء وتكلفة الاكتساب: تفقد الشركات في المتوسط 3.9% من عملائها بعد اختراق البيانات، مع ارتفاع معدل مغادرة العملاء في القطاعات ذات الحساسية العالية مثل المالية والصحة. تكلفة اكتساب عملاء جدد تزداد بنسبة 29% بعد الحوادث الأمنية.

تكاليف الفرص الضائعة: تضطر المؤسسات لتأجيل مشاريع استراتيجية وابتكارية للتركيز على معالجة الاختراق، مما يؤثر على قدرتها التنافسية. تقدر تكاليف الفرص الضائعة بنحو 23% من إجمالي تكلفة الاختراق.

التكاليف الاقتصادية لسرقة الهوية واختراق البيانات: تفرض سرقة الهوية تكاليف اقتصادية ليس فقط على الأفراد، بل أيًضا على الشركات والحكومة، للوقت الذي يقضيه الضحايا في حل المشاكل الناجمة عن الاحتيال على الهوية والتكاليف التي يتحملها الضحايا لحل الجريمة والتي قد تشمل الرسوم القانونية والأجور المفقودة ودفع أي ديون احتيالية ونفقا ت أخرى مثل رسوم البريد والتصديق، بلغ إجمالي المبلغ الذي سرقه سارقوا الهوية من الضحايا في الولايا ت المتحدة حوالي 18مليار دولار في عام .2013

أظهرت دراسة معهد بونيمون لعام 2013 حول التكلفة العالمية لاختراق البيانات أن القطاع الذي تكبد أعلى تكلفة في عام 2012 كان قطاع الرعاية الصحية (233 دولاً را لكل سجل مفقود يليه القطاع المالي 215 دولارا لكل سجل مفقود وصناعة الأدوية 207 دولارا لكل سجل مفقود. وكان قطاع التجزئة في أدنى مستوى بتكلفة اختراق بيانات تبلغ 78دولارا لكل سجل مفقود

التكاليف البشرية لسرقة البيانات

تكاليف التوظيف والتدريب: تتطلب معالجة الاختراقات توظيف خبراء إضافيين بتكلفة عالية. يجب إعادة تدريب الموظفين بتكلفة تزيد عن 50,000 دولار للمؤسسة.

تغييرات في القيادة: 60% من مديري تكنولوجيا المعلومات ومسؤولي أمن المعلومات يغادرون مناصبهم خلال ستة أشهر من اختراق كبير.

إرهاق فريق تكنولوجيا المعلومات: يعمل موظفو الأمن السيبراني ساعات إضافية لأسابيع أو شهور بعد الاختراق. يؤدي هذا إلى إرهاق وإجهاد كبير.

شهدت التكلفة العالمية للجرائم الإلكترونية زيادة مطردة خلال السنوات الماضية، متجاوزة توقعات الخبراء. بلغت الخسائر العالمية من الهجمات السيبرانية 6.9 تريليون دولار في عام 2022، وهو ما يعادل حوالي 8% من الناتج المحلي الإجمالي العالمي.

تشير التوقعات إلى أن هذه التكلفة ستستمر في الارتفاع لتصل إلى 10.5 تريليون دولار سنوياً بحلول عام 2025، مدفوعة بالتوسع في الاقتصاد الرقمي وتزايد تعقيد الهجمات .هذا المبلغ يتجاوز القيمة السنوية لتجارة المخدرات العالمية وجميع الكوارث الطبيعية مجتمعة.

استخدام للذكاء الاصطناعي في مجال الأمن السيبراني[13]:

يُستخدم الذكاء الاصطناعي حاليًا في مجال الأمن السيبراني في العديد من التطبيقات، بما في ذلك الكشف عن التهديدات، وتحليل السلوك، واكتشاف الشذوذ، والاستجابة الآلية للحوادث. تُمكّن الأدوات المُدعّمة بالذكاء الاصطناعي المؤسسات من تعزيز دفاعاتها ضد التهديدات السيبرانية المُعقدة من خلال توفير مراقبة آنية، وتحليلات تنبؤية، وتدابير أمنية تكيفية. علاوة على ذلك، يُستخدم الذكاء الاصطناعي لتبسيط العمليات الأمنية، وأتمتة المهام الروتينية، وتعزيز قدرات مُختصي الأمن السيبراني. ومع تطور التهديدات السيبرانية، سيكون للذكاء الاصطناعي دورٌ أساسي في تعزيز الدفاعات الرقمية والتخفيف من المخاطر في ظل بيئة تهديدات متزايدة التعقيد.

فوائد استخدام الذكاء الاصطناعي [14]:

يوفر استخدام الذكاء الاصطناعي في مجال الأمن السيبراني فوائد عديدة، بما في ذلك تعزيز قدرات الكشف عن التهديدات، والكشف الفوري عن الشذوذ، والتحليلات التنبؤية لتحديد المخاطر الأمنية المحتملة والتخفيف من حدتها. يُمكّن الذكاء الاصطناعي من أتمتة مهام الأمن الروتينية، مما يُتيح للموارد البشرية القيام بعمليات أمنية أكثر استراتيجية وتعقيدًا. علاوة على ذلك، يمكن للأدوات المدعومة بالذكاء الاصطناعي التكيف والتعلم من التهديدات المتطورة، مما يوفر تدابير دفاعية استباقية ضد الهجمات السيبرانية المتطورة. بالإضافة إلى ذلك، يُعزز الذكاء الاصطناعي كفاءة وفعالية الاستجابة للحوادث، مما يُقلل من أوقات الاستجابة ويُقلل من تأثير الخروقات الأمنية.

الاستثمار المطلوب في الأمن السيبراني

10-14% النسبة الموصى بها للإنفاق على الأمن السيبراني من ميزانية تكنولوجيا المعلومات

$3750 متوسط الإنفاق على الأمن في الشركات المتوسطة لكل موظف سنوياً

3:1 العائد على الاستثمار كل دولار في الوقاية يوفر 3 دولارات في تكاليف الاختراق

تأمين البنية التحتية الأساسية:

حماية الشبكة: تطبيق جدران الحماية المتقدمة ومراقبة حركة الشبكة. استخدام تقنيات الكشف عن التسلل والتصدي له.

حماية البيانات: تشفير البيانات الحساسة. تطبيق المصادقة متعددة العوامل. تنفيذ سياسات الوصول الآمن.

أمن الخوادم والأنظمة: تحديث مستمر للبرمجيات. تطبيق سياسات الصلاحيات المحدودة. إجراء فحوصات الثغرات بانتظام.

أمن التطبيقات: اختبار أمان التطبيقات قبل الإطلاق. مراجعة الشفرة المصدرية. معالجة الثغرات بسرعة.

[13] Ponemon institute, state of AI in cybersecurity report 2024, p : 12.
[14] IBID, p : 22.

تثقيف وتدريب الموظفين.

وضع استراتيجية وطنية للبيانات.

تطوير الإطار التشريعي.

الاستثمار في البنية التحتية.

بناء القدرات البشرية: تمثل فجوة المهارات في مجال الأمن السيبراني تحدياً اقتصادياً كبيراً، حيث يؤدي النقص العالمي للمتخصصين المؤهلين إلى زيادة مخاطر الهجمات وارتفاع تكاليف التوظيف. وصل متوسط الراتب السنوي لمدير الأمن المعلوماتي (CISO) إلى 280,000 دولار، بزيادة 17 % عن العامين الماضيين.

تقدر التكلفة الاقتصادية لفجوة المهارات بنحو 175 مليار دولار سنوياً، نتيجة لتأخير تنفيذ مشاريع الأمن الحيوية وزيادة مخاطر الاختراق وارتفاع تكاليف الاستعانة بالخبرات الخارجية. تستثمر الشركات الآن في برامج تدريب داخلية وشراكات مع المؤسسات التعليمية لسد هذه الفجوة.

التعاون بين القطاعين العام والخاص في مواجهة التهديدات

تعزيز الشراكات الدولية.

الاطار المفاهيمي لأمن المعلومات في دالة الانتاج

تطوير إطار رسمي لفهم الأهمية المحتملة لأمن المعلومات داخل الشركة من خلال تحديد نموذج إنتاجي مصمم على مستوى الشركة. لنفترض أن الشركات أن يكون لديك دالة إنتاج تربط المدخلات المختلفة، مثل رأس المال والعمالة بالناتج .

$$Y_{it} = A_{it} S_{it}^{\alpha^S} K_{it}^{\alpha^K + \sigma S_{it}} L_{it}^{\alpha^L - \sigma S_{it}}$$

حيث يشير Y إلى إنتاج الشركة i في السنة ، t ويشير A إلى الإنتاجية المحايدة للتكنولوجيا، ويشير S إلى أمن المعلومات، ويرمز K إلى رأس المال المادي، ويرمز L إلى خدما ت العمل إن إدراجنا لأمن المعلومات في وظيفة الإنتاج يعكس الدور المتزايد الأهمية المتمثل في الحفاظ على البيانات آمنة ومأمونة في المؤسسات قد يكون أمن المعلومات أهمية الحفاظ على هوية المنظمة وثقة المستهلكين بها ستؤدي الزيادة في s إلى زيادة في الطلب على رأس المال من عوامل الإنتاج. وبهذا المعنى، فإن أمن المعلومات صبح الأمر أكثر أهمية نسب ًيا عندما تكون تكنولوجيا المعلومات عالية المستوى، و هو أمر ذو صلة خاصة لصناعة التكنولوجيا والبرمجيات عدد خروقا ت البيانات، و هو عكس أمن المعلومات[15] .

[15] Measuring the Economic Effects of Data Breaches on Firm Outcomes: Challenges and Opportunities Christos A. Makridis and Benjamin Dean p 13

الخلاصة

أصبحت البيانات المورد الاقتصادي الأكثر قيمة في العصر الرقمي، تتنافس الحاجة للموازنة بين الابتكار وحماية الخصوصية والأمن.

مع استمرار تزايد الخسائر الاقتصادية للهجمات السيبرانية، أصبح من الضروري اعتماد نهج استباقي ومتكامل لإدارة المخاطر السيبرانية. لم تعد حماية البيانات والأنظمة مسؤولية قسم تكنولوجيا المعلومات وحده، بل أصبحت قضية مؤسسية شاملة تتطلب اهتماماً على مستوى مجلس الإدارة والإدارة التنفيذية.

الحكومات والشركات التي تستثمر بشكل استراتيجي في الأمن السيبراني لا تحمي أصولها الرقمية فحسب، بل تعزز أيضاً ميزتها التنافسية وقدرتها على الابتكار في الاقتصاد الرقمي .يجب أن يكون الهدف النهائي هو بناء منظومة رقمية مرنة قادرة على التعافي بسرعة من الهجمات وحماية القيمة الاقتصادية للبيانات والخدمات الرقمية.

حماية البنية التحتية الحيوية: السيطرة على البيانات الحساسة المتعلقة بالأمن القومي والمواطنين.

الاستقلال الاقتصادي: تقليل الاعتماد على مزودي الخدمات الرقمية الأجانب.

القدرة التنظيمية: فرض القوانين والتشريعات المحلية على البيانات.

تعزيز الابتكار المحلي: دعم الشركات المحلية في مجال التكنولوجيا.

تزداد الحاجة للمهارات المتخصصة في مجال البيانات. علماء البيانات ومهندسو البيانات ومحللو الأعمال وخبراء الأمن السيبراني أصبحوا من أكثر التخصصات طلباً في سوق العمل العالمي.