معهد فلسطين لأبحاث الأمن القومي
Palestine Institute for National Security Research

الهندسة الاجتماعية :عندما يصبح الإنسان بوابة الاختراق

تحليل للهندسة الاجتماعية وأساليب استغلال الإنسان في الهجمات السيبرانية، مع عرض أبرز المخاطر وسبل الوقاية والقراءة الاستراتيجية من منظور فلسطيني.

الدكتور عامر أبو هنية

باحث في الأمن السيبراني والذكاء الاصطناعي

مقدمة

لم يعد اختراق الأنظمة الرقمية يعتمد بالضرورة على اكتشاف ثغرة تقنية معقدة أو تجاوز منظومة حماية متقدمة .ففي كثير من الحالات، قد تكون الطريق الأقصر إلى المعلومات والأنظمة الحساسة هي الإنسان نفسه .ومن هنا برزت الهندسة الاجتماعية باعتبارها أحد التهديدات المهمة في البيئة السيبرانية الحديثة، لأنها لا تستهدف الحواسيب والشبكات فقط، وإنما تستهدف طريقة تفكير المستخدم وسلوكه وثقته بالآخرين.

وتقوم الهندسة الاجتماعية على مجموعة من الأساليب التي يستخدمها المهاجم لخداع الإنسان والتلاعب به بهدف الحصول على معلومات خاصة أو صلاحيات وصول أو دفعه إلى تنفيذ إجراء يخدم الهجوم . ويمكن أن تتم هذه العمليات عبر البريد الإلكتروني، أو الرسائل النصية، أو المكالمات الهاتفية، أو وسائل التواصل الاجتماعي، بل وقد تحدث بصورة مباشرة داخل المؤسسات.

تكمن خطورة هذه الهجمات في أن المهاجم لا يحتاج دائمًا إلى التغلب على النظام الأمني بالقوة؛ بل قد يدفع المستخدم نفسه إلى تجاوز الإجراءات الأمنية أو تقديم المعلومات التي يحتاج إليها .ولهذا فإن حماية الأجهزة والأنظمة، رغم أهميتها، لا يمكن أن تكون كافية من دون حماية السلوك البشري أيضًا.

وتطرح هذه الحقيقة سؤالًا استراتيجيًا مهمًا :هل يمكن بناء أمن سيبراني فعال من دون فهم الإنسان الذي يستخدم النظام؟

تجادل هذه الدراسة بأن الإجابة هي النفي؛ إذ إن مواجهة الهندسة الاجتماعية تتطلب الجمع بين التكنولوجيا وعلم النفس، وبين الضوابط التقنية والتوعية والسلوك الوقائي.

من اختراق النظام إلى اختراق الإنسان

أصبحت المؤسسات تعتمد بصورة متزايدة على أنظمة رقمية وشبكات وخدمات متصلة بالإنترنت، وترافقت هذه التحولات مع تطور تقنيات الحماية السيبرانية .إلا أن هذا التطور لم يُنهِ خطر الهجمات التي تستهدف العنصر البشري.

وتختلف الهندسة الاجتماعية عن كثير من أساليب الاختراق التقليدية في أنها تعتمد على إقناع الضحية بتنفيذ الفعل المطلوب بدلًا من فرضه عليها تقنيًا .وقد يستغل المهاجم الثقة أو الفضول أو الرغبة في المساعدة أو الخوف أو الطمع أو الحاجة إلى الحصول على القبول الاجتماعي.

وهنا تظهر المفارقة الأساسية :كلما تطورت الأنظمة الأمنية وأصبحت أكثر تعقيدًا، قد يبحث المهاجم عن المسار الأقل مقاومة، وهو الوصول إلى المستخدم.

فالإنسان لا يعمل وفق قواعد تقنية ثابتة؛ بل يتخذ قرارات تتأثر بالسياق والعاطفة والضغط الزمني والثقة والانطباعات الشخصية .وهذه الخصائص تجعل العنصر البشري مجالًا قابلًا للاستغلال إذا لم تدعمه ثقافة أمنية مناسبة.

كيف تعمل الهندسة الاجتماعية؟

لا تبدأ عملية الهندسة الاجتماعية عادةً بالطلب المباشر من الضحية تقديم معلومات حساسة، بل تمر غالبًا بمراحل منظمة تبدأ بجمع المعلومات وتنتهي بتنفيذ الهدف.

تتمثل المرحلة الأولى في جمع المعلومات عن الشخص أو المؤسسة المستهدفة .وقد يعتمد المهاجم على المعلومات المتاحة عبر الإنترنت أو وسائل التواصل الاجتماعي، إضافة إلى أساليب أخرى للحصول على صورة عن الضحية وبيئة عملها.

ثم تأتي مرحلة بناء العلاقة والثقة، حيث يحاول المهاجم خلق شعور بالألفة أو المصداقية مع الضحية . وقد يتم ذلك من خلال انتحال صفة شخص أو مؤسسة موثوقة أو استخدام معلومات حقيقية سبق جمعها عن الهدف.

بعد ذلك تبدأ مرحلة الاستغلال، حيث يتم توظيف الثقة أو نقطة الضعف النفسية لدفع الضحية إلى تنفيذ إجراء محدد، مثل الكشف عن معلومات أو فتح رابط أو تنزيل ملف.

وفي المرحلة الأخيرة، التنفيذ والانسحاب، يحقق المهاجم هدفه ويحاول إنهاء التفاعل دون إثارة الشك، وقد لا يدرك الضحية أصلًا أنه تعرض لهجوم.

وهذه المراحل توضح أن الهندسة الاجتماعية ليست مجرد رسالة احتيالية عشوائية، بل يمكن أن تكون عملية منظمة تبدأ بالمعلومات وتنتهي بالتلاعب بالسلوك.

لماذا ينجح الخداع؟

تكمن قوة الهندسة الاجتماعية في قدرتها على استغلال مجموعة من العوامل النفسية.

الثقة والإقناع

الثقة من أكثر العناصر التي يعتمد عليها المهاجم .فعندما ينجح في إقناع الضحية بأنه شخص موثوق أو جهة شرعية، تصبح احتمالية استجابتها لطلباته أكبر.

وقد يستغل المهاجم رغبة الفرد في أن يكون متعاونًا أو مفيدًا للآخرين، فيدفعه إلى تقديم معلومات أو اتخاذ إجراء يتعارض مع السياسات الأمنية للمؤسسة.

العواطف

لا يعتمد المهاجم على المعلومات وحدها، بل يعمل على التأثير في الحالة النفسية للضحية .وقد يستخدم الخوف أو الفضول أو الغضب أو الشعور بالذنب أو الحماس أو الرغبة في الحصول على مكافأة.

وتصبح المشكلة أكثر خطورة عندما تتزامن العاطفة مع ضعف القدرة على التحقق، لأن الضحية قد تتخذ قرارًا سريعًا لا تتخذه في الظروف الطبيعية.

الإلحاح وضيق الوقت

من الأساليب المتكررة خلق شعور بأن القرار يجب أن يُتخذ فورًا .وقد يتضمن ذلك التهديد بإغلاق حساب أو فقدان خدمة أو التعرض لعقوبة أو ضياع فرصة.

والهدف من ذلك تقليص الوقت المتاح للضحية للتفكير والتحقق، وتحويل القرار من عملية عقلانية إلى استجابة عاطفية سريعة.

أبرز أساليب الهندسة الاجتماعية

تتعدد الأساليب المستخدمة في الهندسة الاجتماعية، إلا أن التصيد الإلكتروني يمثل أحد أكثرها شيوعًا.

التصيد الإلكتروني

يقوم التصيد على إرسال رسائل تبدو وكأنها صادرة عن جهة موثوقة، بهدف دفع الضحية إلى تقديم معلومات أو فتح رابط أو تنزيل ملف ضار .وقد يكون التصيد عشوائيًا ويستهدف عددًا كبيرًا من

المستخدمين، أو موجّهًا إلى أشخاص محددين، بما في ذلك كبار المسؤولين وأصحاب الصلاحيات المرتفعة.

وتزداد خطورة التصيد الموجّه عندما يمتلك المهاجم معلومات مسبقة عن الشخص المستهدف، إذ يمكنه تصميم رسالة أكثر إقناعًا وأقرب إلى السياق الحقيقي لعمل الضحية.

التصيد الصوتي والرسائل النصية

لا يقتصر الخداع على البريد الإلكتروني .فقد يتم عبر مكالمات هاتفية تنتحل صفة جهات موثوقة، أو عبر الرسائل النصية التي تدفع المستخدم إلى الكشف عن بياناته أو متابعة رابط معين.

الاختراقات المادية

يمكن أن تنتقل الهندسة الاجتماعية من الفضاء الرقمي إلى العالم الواقعي .فقد يحاول المهاجم انتحال صفة موظف أو مزود خدمة للوصول إلى أماكن أو معلومات غير مصرح له بها داخل المؤسسة.

وهذا النوع يوضح أن الأمن السيبراني لا يمكن فصله بصورة كاملة عن الأمن المادي للمؤسسة.

التداعيات الاستراتيجية للهندسة الاجتماعية

الخطأ في التعامل مع رسالة إلكترونية أو مكالمة هاتفية قد يبدو في ظاهره حادثًا فرديًا، لكنه داخل مؤسسة حكومية أو أمنية أو اقتصادية يمكن أن يتحول إلى خطر مؤسسي.

فالحساب الذي يتم الاستيلاء عليه قد يوفر مدخلًا إلى معلومات أخرى، والموظف الذي يكشف بياناته قد يصبح نقطة انطلاق لهجوم أوسع، كما أن المعلومات البسيطة التي ينشرها الأفراد عن أعمالهم وأنشطتهم يمكن أن تساعد المهاجم في بناء صورة عن المؤسسة وأفرادها.

ومن ثم، فإن الهندسة الاجتماعية ينبغي ألا تُفهم بوصفها مشكلة تقنية محدودة، بل باعتبارها مخاطر بشرية ومؤسسية ذات أبعاد أمنية.

وتشير الدراسة إلى أن الدفاعات التقنية التقليدية وحدها غير كافية عندما يكون الهدف هو التلاعب بالعواطف والسلوك البشري، وهو ما يستدعي نهجًا تكامليًا يجمع بين علم النفس وتكنولوجيا المعلومات.

القراءة الفلسطينية :الأمن السيبراني يبدأ من الإنسان

من منظور الأمن القومي الفلسطيني، تكتسب هذه القضية أهمية خاصة؛ لأن المؤسسات الحكومية والأمنية والاقتصادية تعتمد بصورة متزايدة على الأنظمة الرقمية والاتصالات والخدمات الإلكترونية.

ولا تكمن المخاطر فقط في استهداف البنية التقنية، وإنما أيضًا في استهداف الموظفين والمستخدمين الذين يمتلكون صلاحية الوصول إلى الأنظمة أو المعلومات.

وعليه، فإن التعامل مع الهندسة الاجتماعية يجب أن ينتقل من مفهوم توعية المستخدم إلى مفهوم أوسع هو بناء ثقافة وطنية للأمن السيبراني.

وتتطلب هذه الثقافة إدراكًا بأن الموظف ليس الحلقة الأضعف بالضرورة، بل يمكن أن يكون جزءًا أساسيًا من منظومة الدفاع إذا امتلك المعرفة والقدرة على التحقق والالتزام بالإجراءات الأمنية.

كما ينبغي أن تشمل الحماية كبار المسؤولين وأصحاب الصلاحيات الحساسة، لأن استهداف الحسابات أو الأشخاص ذوي الوصول المرتفع قد تكون له آثار أكبر من استهداف مستخدم عادي.

نحو استراتيجية مؤسسية للوقاية

لا يمكن مواجهة الهندسة الاجتماعية من خلال إجراء تقني واحد .فالاستجابة الفعالة تحتاج إلى طبقات متعددة من الحماية.

أول هذه الطبقات هو التوعية والتدريب المستمر .فالمستخدم يجب أن يكون قادرًا على التعرف على مؤشرات الخداع، وفهم أساليب المهاجمين، ومعرفة متى يجب التوقف عن الاستجابة والتحقق من الطلب.

أما الطبقة الثانية فهي المصادقة متعددة العوامل(MFA) ، التي تضيف مستوى إضافيًا من الحماية إلى جانب كلمة المرور .ومع ذلك، تؤكد الدراسة أن المصادقة متعددة العوامل ليست حماية مطلقة، ويمكن أن توجد أساليب لتجاوزها؛ لذلك يجب ألا تُعامل باعتبارها حلًا وحيدًا.

وتشمل الطبقة الثالثة استخدام كلمات مرور قوية وفريدة، وتجنب مشاركة التفاصيل الشخصية الحساسة التي يمكن أن تساعد في الإجابة عن أسئلة الأمان أو تسهيل انتحال الشخصية.

كما ينبغي للمؤسسات أن تعتمد سياسات واضحة للتحقق من الطلبات الحساسة، بحيث لا يكون مجرد وصول رسالة أو مكالمة كافيًا لتنفيذ إجراء مالي أو تقني أو إداري مهم.

وتبرز كذلك أهمية تأمين الشبكات والأجهزة والخدمات المتصلة، وعدم السماح للمستخدمين غير الموثوقين بالوصول إلى الشبكات الرئيسية، واستخدام وسائل الحماية المناسبة للاتصالات والبيانات.

الاستنتاجات

تكشف الهندسة الاجتماعية عن تحول مهم في طبيعة المخاطر السيبرانية :فالمواجهة لم تعد تدور فقط بين المهاجم والمنظومة التقنية، بل أصبحت تدور أيضًا بين المهاجم والعقل البشري.

وتشير الدراسة إلى أن نجاح هذا النوع من الهجمات يرتبط بقدرة المهاجم على فهم سلوك الضحية واستغلال الثقة والعواطف والإلحاح والظروف النفسية المناسبة .لذلك فإن تطوير أنظمة الحماية التقنية، رغم ضرورته، يجب أن يترافق مع تطوير الإنسان نفسه باعتباره عنصرًا في منظومة الأمن.

وتتمثل الخلاصة الأساسية في أن الأمن السيبراني الفعال هو منظومة تجمع الإنسان والتكنولوجيا والسياسات، وليس مجرد برامج وأجهزة حماية.

توصيات استراتيجية

1. اعتماد برامج مؤسسية مستمرة للتوعية بالأمن السيبراني بدلًا من الاكتفاء بمحاضرات دورية محدودة، مع التركيز على المحاكاة العملية لسيناريوهات التصيد والهندسة الاجتماعية.
2. إجراء تدريبات متخصصة لكبار المسؤولين وأصحاب الصلاحيات الحساسة، نظرًا لأهمية الحسابات والمعلومات التي يمكن الوصول إليها من خلالها.
3. إقرار سياسات تحقق متعددة المستويات لأي طلب يتعلق بالمعلومات الحساسة أو الصلاحيات أو الإجراءات المالية والإدارية المهمة.
4. تطبيق المصادقة متعددة العوامل على الأنظمة والحسابات الحساسة، مع إدراك أنها طبقة حماية وليست بديلًا عن بقية الإجراءات الأمنية.
5. دمج علم النفس السلوكي في برامج الأمن السيبراني لفهم الأسباب التي تجعل المستخدمين يستجيبون للرسائل الاحتيالية، وتصميم برامج تدريب تعالج السلوك وليس المعرفة التقنية فقط.
6. تقليل كمية المعلومات الحساسة المتاحة للعامة على منصات التواصل الاجتماعي والمواقع الإلكترونية، خصوصًا المعلومات المتعلقة بالهيكل التنظيمي والوظائف والأدوار والصلاحيات.

7. إنشاء آليات واضحة وسريعة للإبلاغ عن الحوادث ومحاولات الخداع بحيث يستطيع الموظف الإبلاغ عن رسالة أو مكالمة مشبوهة دون الخوف من اللوم أو العقوبة.
8. اعتماد نهج أمني متعدد الطبقات يجمع بين التوعية والسياسات الأمنية والمصادقة وإدارة كلمات المرور وحماية الأجهزة والشبكات.
9. إدراج الهندسة الاجتماعية ضمن تقييم المخاطر المؤسسية والوطنية وعدم التعامل معها باعتبارها مجرد مشكلة توعوية تخص المستخدم النهائي.
10. تعزيز التعاون بين الجهات الأكاديمية والأمنية والتقنية لدراسة الأنماط الجديدة للهندسة الاجتماعية وتطوير برامج وقائية تتناسب مع البيئة الفلسطينية.

خاتمة

تؤكد الهندسة الاجتماعية أن التطور التقني لا يلغي العامل البشري في الأمن، بل يجعل فهمه أكثر أهمية . فالمهاجم قد يجد أن الوصول إلى الإنسان أسهل من محاولة تجاوز نظام تقني متطور، ولذلك فإن بناء منظومة دفاع سيبراني فعالة يبدأ من إدراك أن كل مستخدم يمكن أن يكون هدفًا، وفي الوقت نفسه يمكن أن يكون خط الدفاع الأول.

إن التحدي الحقيقي أمام المؤسسات لا يتمثل فقط في امتلاك أدوات أمنية متقدمة، وإنما في القدرة على تحويل المعرفة الأمنية إلى سلوك يومي .ومن هنا تصبح التوعية والتدريب المستمر والسياسات الواضحة والضوابط التقنية عناصر مترابطة في استراتيجية واحدة.

وبالنسبة لفلسطين، فإن تعزيز هذا النهج يمثل جزءًا من بناء قدرة وطنية أكثر نضجًا في مجال الأمن السيبراني، بحيث لا تقتصر الحماية على الأنظمة والأجهزة، بل تمتد إلى الإنسان والمؤسسة والثقافة الأمنية التي تحكم السلوك في الفضاء الرقمي.

المصادر

Guitton, M. J. (2020). Cybersecurity, social engineering, artificial intelligence, technological addictions: Societal challenges for the coming decade. Computers in Human Behavior.

Fatima, S. & Naima, K. (2019). Social Engineering Attacks: A Survey. School of Electrical Engineering and Computer Science, University of North Dakota.

Francois, M., Mercia, M., Louise, L. & Venter, H. S. (2014). Social Engineering Attack Framework. Defence Peace Safety & Security, Council for Industrial and Scientific Research, South Africa.

Jansson, K. & von Solms, R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584–593.

Harrison, S. E. (2023). Beyond Phishing: Understanding Social Manipulation Online. In K. L. Adams (Ed.), Digital Defense: Current Strategies.

Venkatesha, S., Rahul Reddy, K. & Chandavarkar, B. (2021). Social Engineering Attacks During the COVID-19 Pandemic. SN Computer Science.

Martin, E. R. & White, L. H. (2023). The Art of Deception: Unraveling Social Engineering Tactics. International Journal of Cybersecurity Education, 6(3), 112-125.

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. 2nd ed., Wiley.

Talamantes, J. (2014). The Social Engineer's Playbook: A Practical Guide to Pretexting.