الهندسة الاجتماعية وارتباطها بالهجمات السيبرانية

غاده بن ربيعان

- **مقدمة في الهندسة الاجتماعية**

في عام 1911 م نشـر عالم الاجتماع إدوارد إيرب كتابًا بعنوان "المهندس الاجتماعي" كوسـيلة لتشـجيع الناس على التعامل مع العلاقات الاجتماعية بشـكل مشـابه للطريقة التي يتعاملون بها مع الأجهزة من حيث الأمان والسـرية. وفي عصـرنا الحديث تعرف الهندسـة الاجتماعية بأنها فن اختراق العقول والتلاعب بالبشـر وخداعهم عن طريق الأنشـطة الخبيثة التي يتم عملها من خلال التفاعل البشـري، مثل: خداع المسـتخدمين لارتكاب أخطاء أمنية أو الكشـف عن معلومات حساسة وذلك لأجل التخريب، التعطيل، أو إتلاف البيانات لإحداث ضرر أو للحصول على معلومات مهمة كالمعلومات الشخصية والبيانات البنكية.

- **الهجوم باستخدام الهندسة الاجتماعية**

تعتمد معظم الهجمات السيبرانية باستخدام الهندسة الاجتماعية على التواصل الفعلي بين المهاجمين والضحايا؛ حيث يميل المهاجم إلى تحفيز المستخدم على تعريض نفسه للخطر بدلاً من استخدام أساليب القوة لخرق البيانات. عادةً ما تتم عملية الهجوم باستخدام الهندسة الاجتماعية بجمع المعلومات الأساسية عن الضحية أو عن المجموعة التي ينتمي لها، ثم تحديد خطة الهجوم والوسائل التي يمكن استخدامها في الهجوم من أدوات معنوية وتقنية، بعدها يتسلل المهاجم من خلال البدء بالتخاطب وتكوين علاقات مع الضحية، فيتم استغلال الضحية بمجرد أن تنشأ الثقة بينهم لبدء الهجوم باستخدام المعرفة المكتسبة .وأخيرًا، الانسحاب من الاختراق دون آثار من خلال حذف البرامج الخبيثة وإخفاء الآثار التقنية والمعنوية ؛ و يمكن أن تتم هذه العملية في رسـالة بريد إلكتروني واحدة أو على مدار أشـهر من خلال وسـائل التواصل الاجتماعي.

- **من أهم أساليب الهندسة الاجتماعية**

1. التصيد الاحتيالي **(Phishing)**: حيث يتظاهر مهاجمو التصيد الاحتيالي بأنهم مؤسسة أو فرد موثوق به لمحاولة إقناع الضحايا بالكشف عن البيانات الشخصية ويتم استهداف الضحايا بالغالب بطريقتين؛ الطريقة الأولى هي التصيد الجماعي، وهو هجوم واسع النطاق يستهدف العديد من المستخدمين ومحاولة القبض على أي شخص. أما الطريقة الثانية هي التصيد بالرمح أو بما يسمى بصيد الحيتان، ويتم عن طريق استخدام المعلومات الشخصية لاستهداف مستخدمين معينين. تستهدف هجمات صيد الحيتان غالبًا المشاهير والإدارة العليا وكبار المسؤولين الحكوميين.
2. الطعم **(Baiting)**: وهو استغلال الفضول الطبيعي للأفراد لإقناعهم بتعريض نفسهم للمهاجم، مثل: وضع أجهزة متنقلة خارجية مثل (USB) تحتوي على برامج ضارة في أماكن عامة وانتظار وقوع الضحايا في الفخ.
3. اتباع الخطى **(Tailgating)** : ويعني تتبع شخص مخول له بالدخول لكي يقتنص الفرصة عند وجود ثغرة.
4. الادعاء أو انتحال الشخصية **(pretexting)** و هو ادعاء المهاجم بأنه شخصية معروفة للضحية للحصول على معلومات بطريقة مباشرة أو غير مباشرة.

- **لماذا يلجأ أغلب المهاجمين إلى استخدام الهندسة الاجتماعية ؟**

يستخدم أغلب المهاجمين أساليب الهندسة الاجتماعية لسهولة إعدادها وتنفيذها كونها لا تحتاج إلى تقنيات متقدمة، بالإضافة إلى قلة الحماية والوعي بها لأن أغلب المنظمات تركز على جودة الأجهزة وأنظمة الحماية ولكن التركيز

على وعي وحرص الموظفين أمر صـعب. أيضًـا، صـعوبة الكشـف و التعقب كونها تعتبر من الجرائم خالية الآثار وتعتمد على استجابات الضحايا للمهاجم .

- **كيفية التصدي لهجمات الهندسة الاجتماعية**

يتطلب من الأفراد التصـدي لهجمات الهندسـة الاجتماعية بممارسـة الوعي الذاتي عن طريق تقييم أنفسـهم من خلال الأسئلة التالية:

- **هل اشتدت مشاعري؟** عندما يكون الشخص فضولي، خائف، أو متحمسًا بشكل خاص، فمن غير المرجح تقييم عواقب الأفعال وسيندفع للأمر دون تفكير.

- **هل جاءت هذه الرسالة من مصدر موثوق؟** فحص عناوين البريد الإلكتروني وملفات تعريف وسائل التواصل الاجتماعي بعناية عند تلقي رسـالة غريبة، بالإضـافة إلى الحرص على عناوين البريد الالكتروني لأنها قد تكون هناك أحرف محاكيه لبريد الإلكتروني الخاص بالمستخدمين، مثل "ghadh@example.com" بدلاً من "ghada@example.com".

- **هل قام صديقي بالفعل بإرسال هذه الرسالة لي؟** الحذر من الحسابات الشخصية المزيفة على وسائل التواصل الاجتماعي التي تكرر صورة معارفك وبياناتهم، ومن الجيد دائمًا سؤال المرسل شخصيًا عما إذا كان هو المرسل الحقيقي للرسالة المعنية سواءً كان زميل عمل أو صديق مقرب.

- **هل يحتوي موقع الويب الذي أستخدمه على تفاصيل مريبة؟** يمكن أن تكون الاختلافات في عنوان الرابط الخاص بالموقع (URL)، رداءة جودة الصور، أو استخدام شعارات للشركة قديمة أو غير الصحيحة، وتعد الأخطاء المطبعية لصفحات الويب بمثابة إنذارات للفرد بأنه يدل على موقع ويب احتيالي. إذا قام الفرد بدخول على موقع ويب مخادع، فيجب عليه مغادرة الموقع على الفور.

- **هل يستطيع المرسل إثبات هويته؟** إذا لم تكن هناك إمكانية في التأكد من أن المرسل ينتمي فعليًا للمنظمة التي يدّعي أنه جزء منها، فلا تسمح له بالوصول لطلبه. ويندرج هذا على جميع وسائل التواصل، مثل: التواصل الشخصي أو عبر الإنترنت.

فتعزيز نظرة المجتمع على مفهوم الهندسـة الاجتماعية أمر مهم لجميع فئاته، فالفئة الأقل تطلعًا بالتقنية وعالم الاحتيال الحديث هم الأكثر عرضة وبشكل مباشر لتلك الهجمات السيبرانية ويعد ذلك أمرًا في غاية السهولة مقارنة بالأشخاص الذين يملكون علم كافي حول تلك المفاهيم التقنية.