- **مقدمة:**

- منذ بداية انتشار فايروس كورونا واجهت منظمة الصحة العالمية زيادة في اختراقات الفضاء السيبراني التي واجهت المنظمة بشكل مباشر وواجهت أيضا حسابات البريد الإلكتروني لموظفيها.
- هذا الأسبوع حوالي 450 عنوان بريد إلكتروني مع كلمات المرور الخاصة بها تم تسريبها بالإضافة إلى آلاف الحسابات الأخرى المرتبطة بموظفين آخرين يعملون ضمن الاستجابة والتصدي لفايروس كورونا تم تسريبها أيضاً.
- التسريبات لم تضع أنظمة منظمة الصحة العالمية في خطر لأن البيانات لم تكن حديثة. ولكن الهجوم أثر على أنظمة أخرى أقدم مستخدمة من قبل الموظفين الحاليين والمتقاعدين وكذلك أنظمة الشركاء.

التحديات التي تواجه الشركات للتصدي لهذه الهجمات

- تضطّر الشركات في مثل هذه الظروف إلى تغيير طريقة عملها (حيث سيمارس الموظفون مهامهم عن بعد ويتم تقديم خدمات الشركة عبر الانترنت) مما يتطلّب التغيير في بنيتها التحتية الخاصة بتكنولوجيا المعلومات والاتصالات.
عندما يحصل اختراق لشركة في الظروف العادية، تقوم الشركة بعملية منظّمة تبدأ بمعالجة هذا الاختراق ومن ثم تحليل المخاطر risk analysis، والاختبار الأمني security testing وأخيراً كيفية مواجهة هذا الاختراق في المستقبل، لكن عند حصول اختراقات متكررة فإنّها ستقوم بمعالجة سريعة لهذه الاختراقات وفق خطوات غير منظمة ومراقبة مما يسبّب تدهور السياسة الأمنية المتبعة في الشركة ويجعل نظامها الأمني سهل الاختراق ومدراء هذه الأنظمة غير قادرين على تحديد نقاط الضعف، وبمرور الوقت عند عدم مطابقة السياسة الأمنية التي تم تحديدها والتحقق من صحتها سابقاً ومع ماتمّ تنفيذه حالياً عند معالجة الاختراقات يسبب ذلك ظهور ثغرات أمنية عالية المستوى critical vulnerabilities.
- تم تغيير البنية التحتية في الشركات بما يتلائم مع مواقع العمل البديلة مما يتطلّب تأمين قنوات اتصال مقدّمة من طرف ثالث واستخدام الخدمات السحابية cloud services، الصعوبة تكمن في ضمان فعالية التحكم الآمن في تنفيذ هذه الخدمات ومراقبتها بالإضافة الى صعوبة في إعطاء الأولوية لتأمين موارد النظام الأمني مما يسبب إهمال الشركة لأمن خدماتها.
- في ظل الوباء يضطّر غالبية الموظفين إلى استخدام أجهزتهم الشخصية (التي قد لا تكون مجهزة أمنيا كما يجب) بسبب نقص الدعم الفني لحل المشكلات المتعلقة بأجهزة الكمبيوتر المحمولة التي توفّرها الشركة ،واستخدام الشبكات المنزلية والعامة الأقل أماناً وبالتالي تحوّلت أنماط الهجوم من اكتشاف طرائق جديدة لاستغلال الثغرات الغامضة الى استغلال ثغرات معروفة ضمن الشبكات المنزلية مما يعني توفر إمكانيات جديدة لاختراق شبكة الشركة.

الشركات المستهدفة :

- مصانع الأغذية
- تجار التجزئة
- المستشفيات بما فيها مخابر الأبحاث الدوائية، مختبرات أبحاث اللقاحات، مديري التجارب السريرية، الصناعات الدوائية.

أمثلة اختراقات أمنية

- **الاختراق الأول:**
- **القضية: القطاع المالي (التأمين)**

- الحادث:
- تم تنفيذ هجوم Spear Phising ، حيث قضى المهاجم بعض الوقت في تعلم أسلوب التمويل في الشركة وشركاءها التجاريين وأنماط الشراء. ثم قام بإرسال فاتورة معدة بشكل جيد لتسليم بعض المنتجات والخدمات من خلال سلسلة من رسائل البريد الإلكتروني من خلال انتحال عناوين المرسل والاستفسارات اللاحقة للتحقق من طلب الدفع.
- التأثير: كانت الخسارة أكثر من 150.000 دولار أمريكي.
- تحليل الهجوم:
- بعد إجراء عمليات تحليل الأدلة الرقمية forensics تبيّن وصول عدد كبير من رسائل التصيد كما اعترف بعض الموظفين ممن استلموا تلك الرسائل أنهم شعروا بأنّ هناك شيء غير طبيعي وأنّهم تجاهلوها بسبب ضغط العمل أحياناً وصعوبة الوصول إلى موظفي الخدمات المعلوماتية علماً أنّ الشريك التجاري الذي تمّ انتحال هويته هو أيضاً ضحية.
- المعالجة Corrections/Improvement:

من أجل التصدي لمثل هذه الاختراقات في المستقبل قامت الشركة بتنفيذ آليات تصفية لرسائل البريد الإلكتروني بالإضافة الى التوعية الأمنية للموظفين لمثل هذه المخاطر.

- **الاختراق الثاني:**
- **القضية: القطاع المالي(البنك) والسلع الاستهلاكية.**

- الحادث: عدوى برامج الفدية (Ransomware) (Ryuk and BeijingCrypt) حيث تم الهجوم الأولي باستخدام هجمات القوة الغاشمة brute force RDP ورسائل البريد الإلكتروني للتصيد spear phishing emails

- التأثير Impact:

تم تشفير البيانات الموجودة على عشرات الخوادم وتعثرت العمليات التجارية لعدة أيام.

العوامل المؤثرة بارتفاع عدد الهجمات

- **أولاً: سلوك المستخدم**

- زيادة استخدام مواقع التواصل الاجتماعي مما يسبب زيادة في عدد الحوادث الأمنية المتعلقة بهجمات التصيد والهندسة الاجتماعية عبر هذه المواقع.
- زيادة في عقد المؤتمرات الفيديوية مع نقاط الضعف المتعلقة بها والمعلومات التي يمكن تسريبها بدون قصد من خلال هذه المؤتمرات.
- زيادة تصفح المقالات المتعلقة بفايروس كورونا لعام 2019 حيث قام المهاجمون باستغلالها من خلال نشر مقالات وأخبار مزوره على مواقع إلكترونية تابعة لهم والتي تم تنفيذ الهجمات من خلالها.

- انتشار مفهوم العمل من المنزل مع نقاط ضعف الشبكات المنزلية.

- **ثانياً: فرص جديدة للجرائم**

- ظروف العمل من المنزل التي فرضها الوباء تفتح أمام المجرمين فرص جديدة للاستغلال فهم على معرفة أن هجمات التصيد والاستغلال التي لم تعد فعالة مع الشركات الكبيرة المحصنة هي فعالة وقابلة للاستغلال في الشبكات المحلية المنزلية.

- **ثالثاً: العامل البشري للعمليات الأمنية وموظفي الاستجابة للطوارئ المعلومات**

- على عكس الموظفين العاديين الذين اختارو العمل من المنزل أو تقليل ساعات العمل خلال فترة الحجر الصحي فإنّ موظفي الاستجابة للطوارئ المعلوماتية كان من الضروري بقاء عملهم بدوام كامل وربما دوام إضافي لزيادة عمليات التحليل والاستجابة للتنبيهات ويضطرون أحيانا للعمل ضمن موقع العملاء مما يستلزم مزيدا من العناية والتعرض لخطر الإصابات.
- قد تقلص الشركة أحيانا من نشاطاتها ويقل الوصول إلى موارد المؤسسة مما يعطي شعورا بالراحة والأمان ولكن بحالة الجائحة زاد الخطر على الموارد بسبب المستخدمين النهائيين الذين يعملون من المنزل بعيدًا عن آليات المراقبة والكشف.

- **رابعاً: فهم القيود الخاصة**

- على الشركات أن تركز على نقاط الضعف المرئية للخارج والتي يمكن للمهاجمين استغلالها لا أن تركز فقط على حماية المعلومات والموارد الداخلية.
- كما يمكن أن يتم تداول معلومات عن الثغرات الأمنية وبيعها وتناقلها وقد تستخدم كجزء من حملات استغلال طويلة الأمد.

الحلول

- **أولاً: تأسيس الخط الجديد**

- كون الموظفين يعملون عن بعد فعلى الشركات أن تراقب هذه المنهجية الجديدة في العمل.
- إذا قررت الشركات الانتقال طويل الأمد إلى العمل عن بعد فعليها تأسيس مايلزم من أنظمة مراقبة وتجهيزات وأجهزة تنبيه خاصة بهذا النمط من العمل.
- قد يستخدم بعض الموظفين شبكات VPN للوصول إلى خدماتهم والمعروف أن هذه الشبكات لديها نقاط خروج جغرافية متنوعة فإذا اتصل المستخدم بشبكة الشركة من جهة أجنبية فقد يؤدي هذا إلى تنبيه يجب التحقيق فيه.

- **ثانياً: تحسين استعداد فريق الاستجابة للطوارئ المعلوماتيّةCSIRT**

الموظف أثناء عمله من المنزل يكون أقل وعياً وتركيزا بيما يمكن للمهاجم أن يستغله خلال فترة انشغاله لذا يجب تحسين الوعي لدى الموظفين بكل ما يتعلّق بالهجمات التي يمكن أن يتعرضوا لها أثناء العمل من المنزل.

أ. **منع الحوادث**

- يجب تحديد المستخدمين الأكثر عرضة للمخاطر ضمن الشركة ومراقبتهم بحثاً عن حالات شاذة مثل التحميلات الكبيرة لبيانات المؤسسة لتحديد الانتهاكات الأمنية المحتملة.
- التأكّد من أنّ المستخدمين يمكنهم التفاعل بسهولة مع فرق الأمن الداخلي بحيث يمكنهم طرح الأسئلة بسرعة عند عدم التأكد من المشكلات المتعلقة بالأمان والإبلاغ عن الحوادث في الوقت الفعلي وأيضاً يجب إبلاغهم بالممارسات الأمنية الجيدة.
- تذكير المستخدمين دائماً باستخدام الأدوات المعتمدَة في المراسَلة ونقل وإدارة المستندات.

ب. زيادة فعالية فريق CSIR ودعم نشاطات المستخدمين

- يجب ضمان أن فريق CSIR مع فريق الخدمات المعلوماتية يجب أن يكون دائماً داعمين لنشاطات المستخدمين الذين يعملون من المنزل ويشكلون خط الدفاع الأول لنشاطاتهم ومتواجدون باستمرار دون انقطاع.

ت. التحكم في الوصول من خارج الشركة

- يجب التأكد من اختبار جميع إمكانيات الوصول عن بعد ومراقبتها باستمرار.
- تخصيص موارد إضافية لضمان أمان النقاط الطرفية التي يستخدمها الموظفون عن بعد.
- تنفيذ مراقبة إضافية على الوصول إلى تطبيقات الشركة التي تخزن المهام الحرجة أو المعلومات الشخصية خاصة من قبل الأجهزة المملوكة شخصيا.
- إيلاء المزيد من الاهتمام والدعم للموظفين الذين لم يتمكنوا من تجنب استخدام اجهزتهم الشخصية من خلال فحص هذه الأجهزة والتأكد من أنها تتمتع بقدرات كافية لمكافحة البرامج الضارة.
- المصادقة متعددة العوامل ستكون مفيدة أيضاً في زيادة أمان أنظمة الشركات.
- تمكين الموظفين المعتمَدين فقط في الوصول إلى تطبيقات ومعلومات الشركة عن بعد.

ث. المراقبة

- يجب التأكّد من أنّ تجهيزات المراقبة الحالية قادرة على تغطية جميع الخدمات الموسعة.
- إذا كانت الشركات تعتمد على مزودي خدمات أمنية مدارة فيجب التأكد من أنّ المراقبة والسجلات تم تكييفها لمراعاة مشهد التشغيل الجديد.

ج. إجرائية الاستجابة للحوادث

- التأكّد من أنّ برتوكولات الاستجابة للحوادث الخاصة بالمنظمة تعكس ظروف التشغيل الحالية ويتم تحديثها بشكل مستمر.
- التأكّد من تعيين بدائل لجميع أدوار فريق CSIRT ، وأنّ كل فرد لديه إمكانية الوصول إلى الموارد التي يحتاجها ليكون قادرًا على الاستجابة لمعلومات الحوادث الواردة بشكلٍ فعال.

إعداد

م. نوره قادري م. تسنيم حسين