الأمن السيبراني في سلاسل الإمداد

مع تزايد تبادل المعلومات والانتقال السريع للبيانات في عصر التكنولوجيا الحديثة، أصبحت سلاسل الإمداد عرضة لتحديات الأمان السيبراني التي تتطلب اهتماماً خاصاً. يعتبر الأمان السيبراني في سلاسل الإمداد من الجوانب الحيوية التي تؤثر على استقرار وفعالية العمليات التجارية للشركات والمؤسسات.

تشكل سلاسل الإمداد الحديثة نظاماً معقداً يتكامل فيه العديد من الشركاء والجهات المعنية، بدءاً من الموردين ووصولاً إلى المستهلكين. هذا التكامل يفتح أبواباً واسعة أمام التهديدات السيبرانية، حيث تصبح البيانات الحساسة والعمليات التشغيلية عرضة للاختراق والتلاعب

تتعامل سلاسل الإمداد مع تحديات الأمان السيبراني التي تتنوع من هجمات الاختراق إلى التلاعب في البيانات والتشويش على العمليات التجارية. يصبح من الضروري على الشركات والمؤسسات تبني إستراتيجيات قوية لحماية بياناتها ومعلوماتها ضد هذه التهديدات المتطورة.

التقنية "سلاح ذو حدين" فكما لها من منافع كثيرة، فإن لها في المقابل مخاطر أيضاً. ويأتي على هرم هذه المخاطر الهجمات الإلكترونية التي تهدد عمليات سلاسل الإمداد، وتسبب زيادة حجم الإنفاق، وغيرها من الآثار السلبية لهذه الهجمات. لذلك دعت الحاجة إلى وجود أمن سيبراني يحمي عمليات سلاسل الإمداد من الهجمات الإلكترونية، وتبعاتها المؤثرة.

أهمية الأمن السيبراني في سلاسل الإمداد

على الرغم من أن التطورات التقنية ساهمت في تحسن عمل سلاسل الإمداد إلا أنها زعزعت الأمن، وظلت المؤسسات تحت تهديد مستمر للهجمات الإلكترونية بسببها. فقد ذكر رئيس أرامكو السعودية وكبار الإداريين التنفيذيين، أمين حسن الناصر: "أن تحول قطاع الطاقة العالمي نحو الرقمنة يؤدي إلى تقاربٍ متزايد وتداخل بين تقنيات المعلومات وتقنيات تشغيل المعامل والمصانع، وذلك يزيد أيضا من الخطر المحتمل للهجمات الإلكترونية التي تعطل أعمال التصنيع، وما يجب وضعه في الاعتبار هو أن قطاع الطاقة منظومة معقدة، لذلك من الضروري أن تمتد قوة الأمن السيبراني إلى ما هو أبعد من شركات الطاقة الكبيرة لتشمل جميع مزودي الخدمات في جميع أنحاء سلاسل الإمداد." وهذا الخطر يستهدف جميع المنشآت ولا سيما الصغيرة، حيث يمكن للقراصنة الوصول إلى شبكات الشركات الأعلى في سلسلة التوريد، وإزالة منتجاتها من سلاسل الإمداد. وقد تسببت الهجمات الإلكترونية حول العالم في زيادة حجم الإنفاق إلى 96 مليار دولار خلال العام الماضي فقط، بزيادة بلغت نسبتها نحو 8% عن حجم الإنفاق خلال العام قبل الماضي.

ويمكن أن نلخص أهمية الأمن السيبراني في عدة نقاط:

- تعزيز الإنتاجية

إن الحماية الأمنية للخدمات اللوجستية وسلاسل الإمداد تضمن سير الأعمال بصورة مستمرة، وتحد من المخاطر الي تؤدي إلى خسائر مالية فادحة للمنظمات.

مثال: شركة ناشئة تعتمد على خدمات لوجستية لنقل منتجاتها، وتستخدم تقنيات الأمان السيبراني لحماية نظام الإمداد الخاص بها. ذلك يسهم في ضمان استمرار سير الأعمال دون توقف غير مخطط له، مما يعزز الإنتاجية ويقلل من التوقفات التشغيلية غير المتوقعة.

- حماية سمعة المنظمة

الهجمات الإلكترونية الي تحدث تؤثر على مصداقية المنظمة، وتهدد سمعتها وموثوقيتها أمام عملائها؛ مما قد يؤدي إلى قلة الفرص الاستثمارية معها

مثال: هجوم إلكتروني على شركة تقنية يتم اكتشافه والتصدي له بفضل تقنيات الأمان السيبراني. ذلك يحمي سمعة المنظمة أمام عملائها، حيث يظلون على يقين من أمان البيانات والخدمات المقدمة، مما يحافظ على ثقتهم في الشركة.

- الحماية من الهجمات الإلكترونية

مثال: شركة تصنيع تستخدم تقنيات الأمان السيبراني لحماية نظامها اللوجستي الذي يتيح لها متابعة وتحسين سلسلة الإمداد. يساعد الأمان السيبراني في تقليل المخاطر المرتبطة بالهجمات الإلكترونية، مما يجعل الشركة أكثر قدرة على الاستفادة من التكنولوجيا بدون مخاوف كبيرة.

للتقنية دور فعال في تحسن سير الأعمال اللوجستية، ولا يمكن أن يستغنى عنها رغم مخاطرها، لذلك أصبح وجود الأمن السيبراني في هذا القطاع مهم؛ حيث بوجوده يمكن لأطراف العملية التجارية استخدام التقنية بأريحية تامة دون مخاوف.

- الاستدامة

تضمن المنظمة استدامة أعمال سلاسل الإمداد لديها من خلال تطبيق أساليب الحماية ضد الهجمات السيبرانية المتوقعة.

الهجمات السيبرانية الشائعة على سلاسل الإمداد ومخاطرها

المقصود بالهجمات السيبرانية على سلاسل الإمداد هي وصول المهاجم إلى شبكة الشركة عبر البائعين الخارجيين، أو الموردين، أو سلاسل الإمداد، ونقل الفيروسات أو أي برامج ضارة أخرى من خلالها. ويمكن توضيح عملية الهجوم بشكل أدق وكما عرّفها موقع (الجزيرة نت) بأنها:"تقنية يقوم فيها الخصم بإيصال تعليمات برمجية ضارة، أو مكوّن ضار، إلى جزء موثوق فيه من البرامج أو الأجهزة، حيث يتمكن المُهاجمون أو المخرّبون من سرقة نظام التوزيع بالكامل الخاص بالبرنامج لتحويل أي تطبيق يبيعونه وأي تحديث برمجي يدفعونه، وحتى المعدات المادية التي يشحنونها للعملاء؛ إلى أحصنة طروادة وذلك من خلال مورد واحد، أي أنه من خلال تدخّل واحد في وضع جيد يمكنهم إنشاء نقطة انطلاق لشبكات عملاء المورد، حيث يصل عددهم أحياناً إلى مئات أو حتى آلاف الضحايا.

وتأتي هجمات سلاسل الإمداد في عدة مشاهد وصور مختلفة، منها:

- هجمات عبر حزم تحديث البرمجيات والأنظمة
في هذا النوع يقوم المهاجم باختراق سلسلة الإمداد وإيصال برامج ضارة من خلال تطبيق واحد فقط أو جزء من برنامج. وغالباً تكون نقاط الدخول من "تحديثات" البرامج والتطبيقات.

- هجمات عبر الأجهزة
والمقصود بها هو استهداف المهاجم أحد الأجهزة للدخول من خلاله، وتهديد أمن سلاسل الإمداد بالكامل وإيصال البرامج الضارة.

- هجمات عبر البرامج الثابتة
إدخال برنامج ضار إلى رمز التشغيل الخاص بالكمبيوتر، ويستغرق تنفيذه ثوان معدودة. حيث بمجرد تشغيل جهاز الكمبيوتر يتم تشغيل البرنامج الضار مما يعرض النظام بالكامل للخطر. كما أن هجمات البرامج الثابتة سريعة، ولا تُكتشف إذا لم يُبحث عنها. وهي ضارة للغاية.

مخاطر الهجمات السيبرانية على سلاسل الإمداد

- أي صناعة ذات إمداد فهي ذات شبكة معقدة يمكن أن تشكل الهجمات الإلكترونية خطراً عليها، وعلى بياناتها. ولكن الخطر الأكبر يكمن في هجماتها على قطاعات الإلكترونيات والتصنيع، حيث تعرضت شركات هذه القطاعات إلى هجمات، وفقدان للبيانات أدى إلى توقف عملها مؤقتاً، وجميع الحركات تتعرض إلى أخطار معنوية، ومادية جرّاء حدوث تلك الهجمات.
  - فقدان بيانات العملاء الحساسة.
  - سرقة وبيع المعلومات من المؤسسة.
  - الضرر بسمعة الشركة.
  - تعطيل عملية التصنيع.
  - إتلاف البيانات والأجهزة.
  - زيادة حجم الإنفاق على تكاليف الأمن والحماية.

مبادرات سعودية لتأمين سلاسل الإمداد

في هذا الصدد ساهمت العديد من المؤسسات السعودية في إطلاق عدة مبادرات من شأنها الحد من خطر الهجمات الإلكترونية وتأمين سلاسل الإمداد، منها:

- مبادرة جسري
مبادرة أطلقها سمو ولي العهد الأمير محمد بن سلمان- حفظه الله- في عام 2021م، بهدف تطوير إستراتيجية موحدة لاستقطاب سلاسل الإمداد العالمية إلى المملكة، وجذب استثمارات نوعية بقيمة 40 مليار ريال سعودي خلال السنتين الأولى من إطلاق المبادرة، حيث تم تخصيص ميزانية للمبادرة بقيمة 10 مليارات ريال سعودي لتقديم حزمة واسعة من الحوافز المالية وغير المالية للمستثمرين.
- برنامج Security Pass
يهدف هذا البرنامج إلى تأمين وحماية المؤسسات والشركات الي تخدم شركة STC، ويركز عى الموردين باعتماد أفضل ممارسات الأمن السيبراني عبر المعايير الصارمة التي يحصلون من خلال تطبيقها على شهادة الامتثال لضوابط الأمن السيبراني.

- شهادة التزام الأطراف الخارجية بضوابط الأمن السيبراني
شهادة أصدرتها أرامكو السعودية في عام 2020م لضمان التزام جميع الأطراف الخارجية لدى أرامكو السعودية لمتطلبات الأمن السيبراني الواردة في معيار أرامكو السعودية للأمن السيبراني للأطراف الخارجية، وذلك لحماية أرامكو السعودية من التهديدات السيبرانية المحتملة وتعزيز الموقف الأمني للأطراف الثالثة.
- تشريعات هيئة المحتوى المحلي والمشتريات الحكومية

وتأتي مبادرة هيئة المحتوى المحلي لتأمين سلاسل الإمداد على عدة تشريعات منها:

1. تشكيل فرق لتنمية المحتوى المحلي.
2. حوكمة وسن ضوابط المحتوى المحلي للشركات المملوكة بالكامل للدولة أو أي من أجهزتها الحكومية أو التي تمتلك فيها الدولة أكثر من (50%) من رأس مالها.
3. إحداث فرص توطين متعددة لمختلف الصناعات، منها: صناعة المنتجات الدوائية، وصناعة منتج الخوادم، وصناعة منتجات السلامة والحماية من الحريق.

- وزارة الاتصالات وتقنية المعلومات
وضعت وزارة الاتصالات وتقنية المعلومات سياسة" الحوسبة السحابية أولاً للمملكة العربية السعودية" بهدف تحديد وتحفيز انتقال القطاع العام من الحلول التقنية التقليدية إلى النماذج القائمة عى الحوسبة السحابية، وتعزيز الأمن السيبراني من خلال اعتماد نموذج الحوسبة السحابية الصحيح لكل هدف. كما تهدف إلى تسريع نمو استخدام خدمات الحوسبة السحابية للجهات الحكومية عند اتخاذ قرارات جديدة للاستثمار في تقنية المعلومات.

- هيئة السوق المالية
أصدرت دليلاً إرشادياً للأمن السيبراني يوضح الضوابط المتعلقة بالأمن السيبراني لمؤسسات السوق السعودية الخاضعة لمتابعة وإشراف هيئة السوق المالية، بهدف تحسين إدارة مخاطر الأمن السيبراني، وفقاً لأفضل الممارسات العالمية وتشريعات الأمن السيبراني المحلية.

- الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)
طورت الهيئة السعودية للبيانات والذكاء الاصطناعي -بصفتها الجهة المسؤولة عن تنظيم البيانات الوطنية- إطار لحوكمة البيانات عى المستوى الوطي، يحدد السياسات الخاصة بتصنيف البيانات، ومشاركتها، وتنظيمها، وطرق الحصول على المعلومات العامة لدى الجهات الحكومية، والبيانات المفتوحة، وذلك لفترة مؤقتة لحين صدور الأنظمة والتشريعات المتعلقة بتصنيف البيانات. بالتالي أصدرت الهيئة وثيقة تدمج جميع السياسيات والتشريعات المتعلقة بحوكمة البيانات.

- البنك المركزي (ساما)

أصدر البنك المركزي "ساما" دليل أو كتيب يتضمن تعليمات عن كيفية إسناد المهام للطرف الثالث، يستهدف البنوك لتوضيح أهمية تبني إطار لإدارة المخاطر المتعلقة بإسناد المهام إلى طرف ثالث، من خلال طريقة تتسم بالسلامة وسرعة الاستجابة.