التكليف النصفي لمقدمة في الإدارة العامة

نسعى إلى تأسيس شركة في خدمات الأمن السيبراني تعمل لخدمة القطاعات الحكومية و الخاصة، و هما في فضاء الأمن السيبراني مرتبطان ببعضهما البعض، إذ أن ضرر الاختراقات أو البرمجيات الخبيثة متعدي إلى جميع الأجهزة و القطاعات إذ أنه لا يوقفها إلا كون نظام الحماية على درجة من القوة للتعرف على الاختراق ثم منعه فالتصدي له، فالتحري عنه و قد تصل لدرجة الرد عليه، طبعا يتم العمل في مرحلة التحري على تحليل الاختراق أو البرمجية الخبيثة التي تمت مواجهتها بحيث يمكن تطوير نظام دفاعي أقوى قادر على التعرف على البرمجيات الخبيثة المشابهة بشكل أسرع و كيفية التصدي لها و منعها من إلحاق أي ضرر.

يعد قطاع الأمن السيبراني ذو حساسية عالية و أهمية كبيرة مع توجه الحكومات إلى رقمنة الحكومة(E-Government) حيث يمكن للمواطن الوصول لوثائقه الشخصية من خلالها، و إنهاء المعاملات، و نصل في بعض الدول إلى كون زيارتك إحدى المديريات يعتبر أمر لحاجة مستعصية، و مع ازدياد عملية الرقمنة من قبل الحكومة تزداد الاختراقات، و عمليات النصب، و الاحتيال عن طريق الحصول على معلومات حساسة عن المواطنين و ابتزازهم بها أو استخدامها لسرقتهم، مما يجبر الدولة عند مرحلة معينة للقيام بحملات للتصدي لها و هذا مثال بسيط لما يمكن فعله عن طريق أبسط عمليات الاختراق، و يجب أن نصحح مفهوم الاختراق إلى كونه ليس بالضرورة أن يكون رقميا فقط، و الأمن السيبراني بحد ذاته قائم على مجموعة من الإجراءات كالتوعية أولا، و الاهتمام بأمن مشغلات الخدمة من نقاط اتصال بالانترنت، و خوادم(Servers)، و أجهزة بالإضافة للاهتمام بمكان تركيبها و تأمينها من سهولة الوصول، و للتعرف على عمليات الاختراق و التصدي لها بطريقة أكثر احترافية يتم العمل على برامج للحماية بشكل عام، و برمجيات خاصة أكثر تخصصا و قوة لحماية المنشأة أو الفرد من الاختراقات و تعرضه للضرر.

أهم أدوار شركات الأمن السيبراني، العمل على نظام لحماية المنشأة من تأسيس البنية حتى الوصول للبرمجيات التي تحتجها الشركة، بالإضافة إلى تجربة الأنظمة التي تم تأسيسها أو الموجودة مسبقا عن طريق تعريضها للاختراقات، و هذا ما يسمى بالاختراق الأخلاقي (Ethical Hacking)، و تقديم التقارير عن نتائج هذه العملية و عن بنية المنشأة في مدى إمكانياتها في التصدي للاختراقات التي تتعرض لها بكثرة و كشف الثغرات، و من الضروري لهذه الشركات أن تقوم بتقديم الاستشارات لمختلف القطاعات لتعزيزها و تطويرها.

قد تعمل بعض الشركات على صناعة برامجها الخاصة و بيعها لمختلف شرائح المستفيدين، أو العمل على برامج خاصة تحت الطلب حسب احتياج المستفيد، و أيضا تتجه بعض الشركات إلى تدريب كوادر المنشآت من باب التوعية أو حتى التدريب التقني للكوادر المتخصصة في المنشآت لتأمينها سيبرانيا.

أهم المهارات الضرورية لشركات الأمن السيبراني، هي الكوادر ذات الخبرة في تأمين أنواع مختلفة من الأعمال، فتأمين مواقع التسوق الالكتروني مختلف عن تأمين المواقع الحكومية، أو مواقع البنوك المرتبطة بالخدمات البنكية، و الاختلاف يكون في قوة جدار الحماية التي نحتاج استخدامه و أنواع الاختراقات التي تستهدف كل مجال مختلف عن الآخر.

من المهم جدا العمل على فريق للتسويق و فريق ا قبل البيع أو قسم المبيعات المسؤول عن عرض خدمات الشركة و أعمالها و المجالات التي يمكن العمل عليها و إبرام الصفقات و الاتفاقات.

وجود الكادر الأكاديمي يتيح الفرصة لرفع جودة العمل و المنتج المقدم من قبل الشركة للمستفيدين و رفع الاستفادة منها إلى أعلى الدرجات.

توفير الفريق القانوني، و الاستفادة من خدمات المستشارين القانونيين في إبرام الاتفاقات، و الصفقات، و العقود، و ذلك لضمان الحقوق، و الأمان للشركة، و المستفيدين.

فريق من المراقبة و التقييم و قد نضمن معهم المحللين حتى يتمكنوا من تقديم خدماتهم للشركة و الاستشارات للمستفيدين مستعينين بالتقنيين في المسائل الأكثر تخصصا.

فريق البحث و التطوير، حتى يكونوا النواة الأساسية في تطوير الأدوات المستخدمة في تقديم الخدمات الأمنية و المساهمة في المجال بشكل عام و على المستوى العالمي.

بشكل عام كشركة تعمل في هذا المجال يجب أن تكون هي أولا قادرة على بناء نموذج في الخدمة التي تقدمها، و العمل على مشاريع متنوعة تكسبها القدرة على التعامل مع أنواع مختلفة من الأعمال باختلاف أنواع الاختراقات و الحالات التي تتعامل معها و هذه هي الخبرة التي تكسبها، أيضا كشركة تعمل في مجال أمني فإن التعامل مع حالات طارئة تحتاج لاستجابة سريعة هو أمر وارد جدا و ضروري، الاهتمام بالكوادر الموظفة لهذا النوع من الخدمات فيه حساسية خصوصا إذا كان العمل مع الجهات الحكومية كبير بحيث توظف الحكومة هذه الشركة للقيام بتقييم مثلا لمنشأة أو قسم محدد لديها.

الجهات التي تتعامل معها شركات الأمن السيبراني غالبا ما تنحصر في الشركات و الجهات الحكومية، من ناحية الشركات تعتمد على حجم الشركة لكن غالبا ما تكون الشركات متوسطة الحجم فما فوق هي الشركات التي تحتاج لخدمات أمن سيبراني متقدمة فتستعين بإحدى شركات الأمن السيبراني، و إذا كانت شركة تقنية فهي الأكثر حاجة للاستعانة بشركات الأمن السيبراني و قد تحتاج لأكثر من واحدة حتى تستطيع تنويع طرق الاختراق لتجربة نظامها الأمني أو قوة برامجها و الاستعانة بأفراد أيضا.

أما ما يخص الجهات الحكومية فغالبا ما تستعين بشركات الأمن السيبراني كمتعاقدين لتأمين بوابات الخدمات الالكترونية و الرامج على الهواتف المحمولة كمثال، تدريب كوادر الوزارات أو المنشآت التابعة لها، يمكن أن تتعاقد أيضا بالعمل على البنية التحتية للمنشآت كمباني و تمديداتها للشبكات، الأنظمة الأمنية، أماكن الخوادم و نوعيتها، الأجهزة و مواصفاتها، برامج، تصل إلى أدق التفاصيل حتى نظام الدخول و الخروج و رحلة الموظف من مدخل المنشأة إلى خروجه، للتفصيل الشركة ستحتاج للتعامل مع الوزارات التي تمتلك خدمات الكترونية، وزارة الداخلية، وزارة الخارجية، وزارة الشؤون البلدية، قد تصل إلى وزارة الدفاع، من المؤكد وجود جهات حكومية أخرى، لكن هذه أبرز الجهات التي عادة ما تستعمل الخدمات الالكترونية و تحتاج إلى تأمينها.

الشركة من الطبيعي أن تتأثر بقرارات الدولة كونها شركة في المقام الأول، و عند نقطة معينة من الانخراط مع الدولة في العمل قد تحصل على تسهيلات و امتيازات، و أيضا سيكون لها تأثير في الجهات الحكومية التي تعمل معها بشكل مباشر مع مراعاة الأهداف و الحدود المرسومة لها من قبل الجهة الحكومية، يصل تأثيرها من الأفراد العاملين إلى حد المسؤول في الجهة الحكومية و المجلس المسؤول، بالتأكيد يتم التأثير من خلال التقارير التي يتم تقديمها بشكل دوري للمراقبة و التقييم، و أيضا مقترحات البحث و التطوير.

الأهداف الشخصية التي تحققت هي بناء هذه الشركة التي تمكنت من بناء نموذج عمل قابل للعمل عليه يحتاج إلى اختبار و تطوير، هذه الشركة قادرة على تقديم مكاسب حقيقية لجميع الأطراف التي تتفاعل معها و بالتأكيد من أهمها الدولة ككل، من ناحية أخذ حصة معرفية على مستوى العالم في هذا المجال، و إضافة فائدة اقتصادية للدولة عن طريق حفظ مواردها و عدم الاستعانة بجهات خارجية، حفظها اقتصاديا من الخسائر الفادحة التي تتسبب بها الهجمات الالكترونية، و أكثر ما يهم هو المشتركة في صناعة قرار الدولة في مجال الأمن و الحرب السيبراني عند نقطة من النقاط بناء على القدرات التي سيتم توفيرها و أيضا تقييمها و تجهيزها بها.