الفقرة الأولى: الجرائم المرتكبة من قبل مقدمي الخدمات والمتعهدين سنتناول كل من الجرائم المرتكبة من قبل مقدمي الخدمات(أولا)، لنتطرق بعدها للجرائم المرتكبة من قبل المتعهدين في(ثانيا). أولا: الجرائم المرتكبة من قبل مقدمي الخدمات حدد المشرع المغربي في إطار المادة 50 من القانون 05. 20 المتعلق بالأمن السيبراني مجموعة من الجرائم، و هو ما قد يشكل عدة أضرار للبنية التحتية ذات الأهمية الحيوية. أي الحصول على تأهيل من لدن السلطة الوطنية ، بالإضافة لسلوك المسطرة القانونية، من قبل مقدم خدمات الإفتحاص دون الحصول على تأهيل، و الشروط التقنية (أ-2) ، ويعتبر أول شرط قانوني أن يؤسس متعهد افتحاص أمن نظم المعلومات في شكل شركة خاضعة للقانون المغربي . وأن يكون كل المفتحصين المقترحين من جنسية مغربية . تعد الشروط التقنية من الأمور الأساسية للحصول على التأهيل، إذ يفترض في مقدم هذه الخدمات دراية دقيقة بكيفية تنفيذ عمليات الافتحاص و هي: توفر المتعهد على خبرة في ميدان افتحاص أمن نظم المعلومات، وأن يتوفر على بنية تنظيمية مخصصة حصريا لافتحاص أمن نظم المعلومات، وأن يتوفر على تأهيل في ثلاثة مجالات افتحاص، من بين المجالات المحددة في الملحق رقم 2 المرفق بالمرسوم التطبيقي، و أن يتوفر على مفتحص واحد على الأقل في كل مجال من مجالات التأهيل المطلوبة . بالإضافة لما سلف يخضع المتعهد لتقييم من قبل أحد الهيئات التي تحددها السلطة الوطنية لهذا الغرض . و في الختام بعد أن يتوفر المتعهد على الشروط القانونية و التقنية المطلوبة، يقوم بإيداع طلب التأهيل لدى المديرية العامة لأمن نظم المعلومات، و من بينها النظام الأساسي للشركة و شهادة تقييدها بالسجل التجاري، بعد أن تمنح السلطة الوطنية للمتعهد التأهيل ، يصبح بإمكانه أن يتعاقد مع أي هيأة أو أي مؤسسة من مؤسسات قطاع الأنشطة ذات الأهمية الحيوية ، من أجل تقديم خدمات افتحاص نظم المعلومات . كما سلف الذكر أن التأهيل من قبل السلطة الوطنية أمر ضروري، ويخضع لشروط قانونية، ومقومات بشرية ذات خبرة في مجال الافتحاص، يعتبر مقدم الخدمة مرتكبا لفعل إجرامي. 2-جريمة تقديم خدمات الأمن السيبراني دون تأهيل إن تقديم خدمات الأمن السيبراني، رهين بتوفر مجموعة من الشروط وسلوك مسطرة قانونية للحصول على التأهيل من لدن السلطة الوطنية. و أيضا إلى جزاء مخالفة هذه الشروط(2-ب). من أجل تقديم خدمات الأمن السيبراني لابد من توفر شروط قانونية و أخرى تقنية. -الشروط القانونية : وهي أن يكون مقدم خدمات الأمن السيبراني مؤسسا في شكل شركة خاضعة للقانون المغربي ، وأن يكون كل المختصين المقترحين من جنسية مغربية . -الشروط التقنية : هناك شروط تقنية كذلك ، وهي أن يتوفر على خبرة في ميدان تقديم خدمات الأمن السيبراني ، وتوفره على بنية تنظيمية ووسائل تقنية مخصصة حصريا لتقديم خدمات الأمن السيبراني ، وأن تتوفر فيهم الخبرة و المؤهلات الازمة المحددة في مرجع متطلبات مقدمي خدمات الأمن السيبراني. المتعلقة بخدمتي رصد وتحليل حوادث الأمن السيبراني وكذا معالجتها ، وكذا تدبيرها ، وعندما تتوفر في مقدم خدمات الأمن السيبراني كل من الشروط التقنية والقانونية ، مشفوعا بمجموعة من الوثائق المتعلقة بما هو قانوني كالنظام الأساسي للشخص المعنوي ، وشهادة تقييد الشركة بالسجل التجاري، وكذا مجموعة من الوثائق وعقود الشغل المتعلقة بالأجراء . ويتم هذا الإجراء على نفقة الطالب . لقد ألزم المشرع المتعهدين بمجموعة من الإلتزامات من أجل ضمان سلامة هذه البنيات من أي حادث سيبراني قد يلحق ضررا بها أو بأنظمتها، أو بسلامة معطياتها. و من بين هذه الإلتزامات نجد الإلتزام بإبلاغ السلطة الوطنية و التقيد بتوجيهاتها، ومقدمو خدمات الإفتحاص ، ملزمون بإبلاغ السلطة الوطنية بكل الأحداث والمخاطر التي من الممكن أن تؤثر على سلامة أمن نظم المعلومات و بهذا يشكل مخالفة ذلك جريمة وفق قانون الأمن السيبراني. 000 إلى 200. أو تأمينه من المخاطر السيبرانية ، من خلال الأحداث التي من الممكن أن تؤثر على أمن نظم المعلومات الخاصة بزبائنهم . وذلك خرقا لأحكام المواد 8و30 و33 من القانون 05. 20. 20 ، ومقدمي الخدمات الرقمية، وناشري منصات الأنترنيت، 3-جريمة عدم التقيد بالتدابير القانونية حسنا فعل المشرع عندما ألزم بمقتضى القانون 05. أ-التدابير القانونية ب-جريمة الإخلال بها سنتطرق لكل من الجرائم المرتبطة بنظم المعلومات في (أولا)، لنعرج بعدها للحديث عن الجرائم المرتبطة بالهيئات والبنيات التحتية ذات الأهمية(ثانيا) أولا: الجرائم المرتبطة بنظم المعلومات سنتناول في هذا الصدد لكل من جريمة عرقلة أو منع عملية الإفتحاص(أولا)، 1)جريمة عرقلة عملية إفتحاص أمن نظم المعلومات كما هو معلوم أن المديرية العامة لأمن نظم المعلومات وهي صاحبة الدور الرقابي، من خلال إجراء عمليات إفتحاص أمن نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية، ولقد اشار المشرع المغربي لهذه الجريمة من خلال المادة 50 من القانون 20. 05 المتعلق بالأمن السيبراني التي تنص على أنه "دون الإخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل يعاقب بغرامة من 100000 إلى 200000 درهم كل من قام بأي وسيلة كانت بعرقلة أو بمنع إجراء عمليات إفتحاص أمن نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية، أوعدم اتخاذ التدابير

Summarized by © lakhasly.com

التقنية والتنظيمية الازمة لإدارة المخاطر، أو منع عملية الإفتحاص التي تقوم بها السلطة الوطنية في حالة عدم وفاء أحد المتعهدين بالالتزامات التي يفرضها القانون عليهم. بالرجوع الى الفقرة الأخيرة من المادة 50 من القانون 05. وامتنع عن تنفيذ توجيهات السلطة الوطنية بعد إخباره بها . ثانيا: الجرائم المنصبة على الهيئات و البنيات التحتية ذات الأهمية الحيوية مما لا شك فيه أن البنيات التحتية ذات الأهمية الحيوية التي تتوفر على نظم معلومات حساس، لذلك خص المشرع المغربي للهيئات والبنيات ، التحتية ذات الأهمية الحيوية بالإضافة إلى الحماية التقنية الحماية الجنائية، من خلال الهجمات السيبرانية

Summarized by © lakhasly.com