

وزارة الاتصالات تكافح الخروقات الإلكترونية القرم: أموال الموازنة لا تكفي لإصلاح الأعطال

تواجه شبكة الاتصالات تشويشا مستمرا نتيجة التدخلات الالكترونية من العدو الاسرائيلي، مما يضعف جودة الخدمات ويهدد الامن الرقمي. ورغم الجهود المبذولة، فهناك معوقات مالية كبيرة، حيث لا تكفي الموازنة الحالية لمواجهة هذه التحديات وتحسين الوضع. هذه الحالة تتفاقم، مما يتطلب دعما وتنسيقا لحماية البنى التحتية للاتصالات لعدم الوقوع في المخاطر

يعتبر اختراق الامن السيبراني تحديا متزايدا في العصر الرقمي، حيث تؤثر الهجمات الالكترونية سلبا على سلامة المعلومات للأفراد والشركات. تتضمن هذه الاعتداءات الوصول غير المصرح به الى الانظمة والشبكات، مما يؤدي الى سرقة البيانات، وتدميرها، او تعطيل الخدمات. ويمكن ان تنجم عنها ثغر امنية، وبرمجيات خبيثة، او تقنيات تصيد احتيالي قد تؤدي الى اضرار كبيرة مثل فقدان المعلومات والتكاليف المالية، وتدهور سمعة المؤسسات. ولأن المطلوب لمواجهة لردع المعتدي، تعتمد وزارة الاتصالات اساليب الحماية مثل التشفير وتحديث الانظمة. اضافة الى ذلك، يعتبر تدريب الموظفين لزيادة الوعي بالمخاطر الامنية امرا اساسيا، فالوقاية والتخطيط المسبق هما اساس مواجهة الاختراقات وحماية الاصول من التهديدات المتطورة.

اما في الونة الاخيرة، فقد اخترقت خصوصية المواطن بعد ان شن العدو الاسرائيلي حربه الالكترونية المبرمجة، لذا كان لا بد من من اعتماد استراتيجيات الامن السيبراني وتطبيق البروتوكولات الصارمة. نذكر منها على سبيل المثال التشفير القوي للبيانات، وتحديث الانظمة لمواكبة التحديات عبر الرصد وتحليل النشاط الشبكي لاكتشاف اي محاولات اختراق او نشاط غير طبيعي. علاوة على ذلك، فان تحسين شبكات الاتصالات من اي تدخلات خارجية اصبح امرا ضروريا.

"الامن العام" اضاءت على الملف، واجرت حوارا مع وزير الاتصالات جوني القرم.

ما هو موقف الوزارة من تطوير تقنيات الجيل الخامس (5G) وهل يمكن تنفيذها في لبنان؟

ان جميع انظمة الاتصالات ضمن شبكات تاتش والفا، تتوافق مع متطلبات الجيل الخامس للاتصالات. وتسعى الوزارة الى تطويرها لتكون جاهزة لتقنيات هذا الجيل، لكن نركز حاليا على تحسين شبكة الالياف الضوئية وتعزيز خدمة 4G من حيث السرعة والسعة قبل الشروع في اطلاق الجيل الخامس بشكل شامل. نقوم بخدمات متقدمة ذات جودة عالية من خلال تحسين البنى التحتية الحالية والانتقال تدريجا الى تقنيات تتوافق مع الاستراتيجيات والخطط الموضوعية.

كيف تتعاون الوزارة مع القطاع الخاص لتعزيز الحماية على الشبكات؟

تتعاون بشكل دائم مع القطاع الخاص لتعزيز الحماية على الشبكات وضمان خدمة عالية الجودة. يتم ذلك من خلال عقد لقاءات دورية مع الشركات المتخصصة في الصيانة، والتأكد من تحقيق معايير المعتمدة. كما يتم رصد الاحتياجات



وزير الاتصالات جوني القرم.

كيف تعمل الوزارة على تحقيق وتوفير الخدمات لجميع المواطنين في ظل ازمة الكهرباء؟

في ظل ازمة الكهرباء المستمرة، تعمل الوزارة على التأكد من صيانة المولدات التي تزود محطات الاتصالات بالكهرباء لضمان استمرارية الخدمة. بالاضافة الى ذلك، يتم الاستفادة من المولدات الخاصة والبطاريات التي توفر الكهرباء بين ثلاث الى ست ساعات، كما يتم التشجيع على استخدام الطاقة الشمسية ايضا. اما بالنسبة الى اوجيرو، فانها تقوم بتنفيذ مشروع الطاقة الشمسية بفضل الهبة الصينية، مما يساعد في تحسين التغذية الكهربائية. وعلى الرغم من الانقطاع المستمر للتيار، ما ارغب في الاشارة اليه، الى انه ومن خلال هذه الاجراءات والحلول البديلة تمكنت الوزارة بالتعاون مع الشركات من توفير استعمال الشبكة بنسبة 95%، مما يساهم في الحفاظ على جودة الخدمة.

”

العدوان اخرج معظم شبكات القرى الحدودية من الخدمة

“

العدوان اخرج معظم شبكات القرى الحدودية من الخدمة بشكل كلي وكامل.

ما هي المبادرات التي يتم تنفيذها لتعزيز الحماية من الرسائل المملوومة عبر الواتساب؟

على المستوى التقني، لا تمتلك الشركات القدرة على التحكم في الرسائل المملوومة التي تصل عبر الواتساب. لذلك، يتم التركيز على التوعية كمبادرة رئيسية للمواجهة. وتنشر الوزارة عددا من المواد التوعوية التي تهدف الى تعليم المستخدمين على كيفية التعامل مع هذه الرسائل، وعدم فتح اي من التطبيقات المحلقة مما يستدعي اعادة تأهيلها بعد اجراء الكشوفات الميدانية عند توفر الهدوء والهدنة. اقول في هذا الصدد ايضا، ان هذا الامر المستجد هو خارج عن اي خطط ملحوظة او متوقعة وسيرتب حكما علينا اعباء اضافية، لأن

الفا، فهناك نحو 60 محطة متوقفة، منها 5 محطات مدمرة كليا. ما ارغب في التصريح به، هو ان الوزارة والشركات تعملان لمعالجة الاعطال واعادة تشغيل المحطات قدر المستطاع بعد الحصول على الموافقات الامنية اللازمة. كما ان المستجندات الاخيرة في الجنوب، اثرت على جودة الاتصالات وذلك بسبب التشويش الحاصل من العدو الاسرائيلي على تردد MHZ900 عندئذ تقوم الشركات باستخدام ترددات بديلة للحفاظ على نوعية الاتصالات. اما بالنسبة الى اختراق نظام GPS فانه يتم اتخاذ اجراءات خاصة مع الشركات لتفاديها.

في هذا السياق، كنا قد تقدمنا بشكوى لدى الامم المتحدة والاتحاد العالمي للاتصالات لمعالجة الموضوع دبلوماسيا. في الخلاصة، ان الحرب الدائرة في الجنوب تعرض بشكل كبير حياة الموظفين للخطر بسبب الاصابات المباشرة المزمع ان تطالهم، اضافة الى الاضرار المادية الكبيرة التي تلحق بالشبكة الهاتفية المحلية مما يستدعي اعادة تأهيلها بعد اجراء الكشوفات الميدانية عند توفر الهدوء والهدنة. اقول في هذا الصدد ايضا، ان هذا الامر المستجد هو خارج عن اي خطط ملحوظة او متوقعة وسيرتب حكما علينا اعباء اضافية، لأن



■ ما هي الاجراءات المتبعة لحماية الطائرات عند الهبوط وهل هناك تواصل مع الجهات الدولية لمنع اسرئيل من استباحة ارواح الناس؟ □ حماية الطائرات عند الهبوط تقع ضمن مسؤولية وزارة الاشغال والطيران المدني اللبناني، وتركز الاجراءات المتبعة على مواجهة التشويش الحاصل على نظام GPS لضمان سلامة الطائرات والركاب. حالياً، قامت وزارة الاتصالات بتقديم شكوى الى الامم المتحدة والاتحاد العالمي للاتصالات عبر وزارة الخارجية في شأن التهديدات الاسرائيلية. وهي تتابع حالياً مع هذه الجهات المعنية الموضوع لضمان حماية الطيران من اي اعتداءات قد تؤثر على سلامة الرحلات. ما اود الاضاءة عليه هو انه يتم التنسيق لاتخاذ الاجراءات اللازمة وضمان استمرارية السلامة في الاجواء اللبنانية. لا بد من الاشارة الى ان الخطط المستقبلية لتحديث القوانين المتعلقة بقطاع الاتصالات يلزمها التشريع وذلك للأسباب التالية: صدور القانون رقم 431 تاريخ 2002/7/23 ولغاية تاريخه لم تصدر المراسيم التطبيقية له. كما ان مرور الزمن على صدوره يستدعي اعادة النظر وتطويره وفقاً للتطورات الحاصلة في هذا القطاع. منذ ذلك التاريخ، وبما ان الحكومة هي لتصريف الاعمال وليس لديها صلاحيات استثنائية والمجلس النيابي لديه الكثير من القوانين لدراستها، فان الوقت الحالي ونظراً الى الظروف الحالية، فهو غير مناسب لاصدار التشريعات اللازمة لمواكبة تطور الاتصالات العالمي. ان صدور القانون المذكور قد منع الوزارة من التوظيف، وحيث ان الكثير من الكوادر الفنية والمؤهلة تبلغ السن القانونية سنوياً، فان المراكز الرئيسية اصبحت شاغرة ولا يمكن تكليف اي فرد وفقاً للمهام للقيام بالمسؤوليات المحددة قانوناً، مما يطرح اشكالية كبيرة لتسيير العمل في المرفق العام. اما بالنسبة الى منع الاختراق، اكرر ايضا ان هذا الموضوع تهتم به الوزارة تحت اشراف رئاسة مجلس الوزراء بالاضافة الى الجهات الامنية المعنية لوضع الخطط اللازمة للامن السيبراني الوطني. بما ان مسؤولية حماية الطيران تقع على عاتق المطار والطيران المدني، فاننا طالبنا الجهات الدولية بالتدخل السريع لمنع تهديد سلامة الطيران وزهق ارواح الناس.



المتعلقة بقطاع الاتصالات انشاء لجنة الامن السيبراني ضمن المجلس النيابي، واطلاق المراسيم التطبيقية الخاصة بها. كذلك يتوجب ايضا وجود هيئة ناظمة للاتصالات ضمن الوزارة لمراقبة القطاع وضمان سلامة البيانات، ويتم العمل على وضع تشريعات جديدة تتماشى مع التحديات الحالية في مجال الامن السيبراني التي تعمل على تعزيز الحماية والمعلومات المهمة.

◀ والتدابير اللازمة لضمان استمرار العمل واصلاح الاعطال الطارئة. ان هذا التعاون يساهم في تعزيز الحماية وضمان استمرارية الخدمة.

■ ما هي الخطط المستقبلية لتحديث القوانين والتشريعات المتعلقة بقطاع الاتصالات ولمنع الاختراق؟ □ تتطلب عملية تحديث القوانين والتشريعات

كيف تحمي نفسك من الرسائل الملوغمة؟

- تحقق من مصدر الرسائل، وتأكد من انها تأتي من مصادر موثوقة وتجنب فتحها اذا كانت الروابط من مرسلين مجهولين او غير معروفين.
- كن حذراً من الروابط المرعبة ولا تنقر على اي رابط مشبوه، حتى لو بدا الرابط موثقاً، وتأكد من صحته من خلال التحقق من عنوان الموقع في المتصفح.
- استخدم برامج حماية وثبتته كما مكافحة الفيروسات والجدران النارية التي تكون سداً منيعاً في وجه الرسائل الضارة والبرامج الخبيثة.
- تحقق من الرسائل قبل فتحها واذا كانت تبدو غير عادية او غير متوقعة، تحقق من محتواها عبر البحث عنها على الانترنت او استشارة الخبراء.
- حدّث البرمجيات بانتظام وحافظ على نظام التشغيل والبرامج والتطبيقات.
- كما يمكنك اتباع هذه الخطوات لتقليل من المخاطر المرتبطة بالرسائل المضللة والحفاظ على امان المعلومات الشخصية، اضافة الى استخدام اجهزة عالية الجودة لتقليل من التأثيرات.