

من الوزير الأول
إلى السادة الوزراء
وكتاب الدولة

الموضوع : حول سلامة النظم المعلوماتية .

المصاحب : استمارة .

يشهد العالم تحولات متسارعة في مجال تكنولوجيا المعلومات بمختلف أشكالها واستعمالاتها وقد حققت تونس إنجازات ومكاسب عديدة في مستوى بناء أنظمة المعلومات وتطويرها ، باعتبارها إحدى الموارد الإستراتيجية وركيزة من ركائز التنمية الشاملة .

وبقدر ما تساهم هذه التقنيات الحديثة في إضفاء مزيد من النجاعة على العمل الإداري والرفع من الإنتاجية والقدرة التنافسية للمؤسسات ، وتحقيق انفتاحها على محيطها الاقتصادي والاجتماعي ، فإن إمكانية تعرض النظم المعلوماتية في مستوى معادتها أو برمجياتها أو معطياتها إلى مخاطر مصيرية واردة على أكثر من مستوى . وتتمثل بعض هذه المخاطر في اقتحام المنظومة دون الحصول على إذن في ذلك أو قرصنتها . وقد يصل الأمر إلى حد تعطيل المنظومة ذاتها ، أو حتى محاولة فسخ أو تزييف محتواها . ولضمان المناعة اللازمة لهذه الأنظمة وحمايتها من كل ما يهددها من مخاطر ، وتوفير الظروف المناسبة للإحاطة بمختلف جوانبها ، يتعين اتخاذ جملة من الإجراءات الكفيلة بضمان سلامة البرمجيات والمعدات وطرق الاستغلال وتراسل المعلومات و تخزينها .

وتتمثل هذه الإجراءات في :

- وضع خطة لسلامة النظم المعلوماتية بالمؤسسة وتطوير برنامج العمل في الغرض . ويمكن الاستئناس في هذا الإطار بدليل منهجي توفره كتابة الدولة للإعلامية ، وتضعه على الذمة ،
- المبادرة بتعيين إطار يكلف بمتابعة سلامة منظومة المعلومات وبالتنسيق مع وحدة تطوير سلامة النظم المعلوماتية بكتابة الدولة للإعلامية .

ونظرا لأهمية الموضوع ، الرجاء من السادة الوزراء وكتاب الدولة إعطاء التعليمات اللازمة للمصالح والمؤسسات والمنشآت الراجعة لهم بالنظر لتطبيق ما جاء بهذا المنشور وتعمير الاستمارة المصاحبة بكل دقة وعناية وتوجيهها إلى كتابة الدولة للإعلامية قبل موفى شهر مارس 2000 .

والسلام ،

وزير الدولة
محمد الحنا
الإمضاء: محمد الغنوشي

استمارة حول سلامة النظم المعلوماتية

التعريف بالمؤسسة

I- الإرشادات العامة :

1- الإدارة أو المؤسسة :

2- اسم المسؤول :

3- العنوان الكامل :

4- الهاتف : الفاكس : البريد الإلكتروني :

II - النشاط :

1- قطاع النشاط :

☐ إدارة

☐ نقل

☐ صحة

☐ مالية

☐ صناعة

☐ خدمات

☐ أخرى (حددوا)

2- وصف النشاط :

3- العدد الجملي للأعوان

إعلاميون منهم

الجواب التنظيمية المرتبطة بسلامة النظم المعلوماتية

I - مخطط السلامة :

☐ لا

☐ نعم

أ - هل أنجزتم مخطط سلامة^١ ؟

1- أنجزه :

☐ فريق مناولة في إطار خدمات

☐ فريق داخلي

2- يمثل جزءا من مخطط مديري :

☐ لا

☐ نعم

3- مخطط السلامة مصادق عليه من طرف :

☐ إدارة عامة ☐ إدارة إعلامية ☐ خبير داخلي ☐ لجنة الاستراتيجية والبرامج والمشاريع والموازن الإعلامية

4- حددوا الفترة الزمنية للإنجاز :

تاريخ البداية :

تاريخ النهاية :

تاريخ البداية :

5- أشيروا إلى المبلغ الجملي المخصص للإنجاز :دينار تونسي

II - إطار متابعة السلامة :

☐ لا

☐ نعم

ب - هل لديكم مسؤول عن السلامة ؟

☐ لا

☐ نعم

1- هل أن مسؤولياته محددة بشكل واضح ؟

2- هل هو على علم بكل حوادث السلامة بالمؤسسة التي قد تكون ناتجة عن فيروسات أو محاولات اختراق الشبكة... ؟

☐ باستمرار

☐ أحيانا

☐ إطلاقا

III - سياسة التحسيس والتكوين :

☐ لا

☐ نعم

ج - هل لديكم سياسة تحسيس وتكوين حول السلامة ؟

1- هل توجد سياسة تحسيس حول المخاطر في صلب المؤسسة ؟

☐ لا

☐ لكل الأعوان

☐ للإعلاميين فقط

2- تنفذ سياسة التحسيس حول المخاطر . من خلال :

☐ أخرى (حددوا)

☐ ملحوظات مكتوبة

☐ تعليمات شفوية

3- هل تلقى إدارت الإعلامية تكوينا في السلامة ؟

☐ بشكل كاف

☐ بقلّة

☐ إطلاقا

^١ في صورة الإجابة بـ "نعم" على هذا السؤال وعلى غيره من الأسئلة الواردة في شكل عناوين فرعية ، فإنه يمكنكم المرور إلى الإجابة عن الأسئلة الموالية الواردة في نفس إطار العنصر .
في صورة الإجابة بـ "لا" ، فإنه يتعين عليكم تجاوز هذا العنصر ، والمرور مباشرة إلى الإجابة عن الأسئلة الواردة في بقية عناصر الاستمارة .

مخاطر فيروسات الإعلانية

1- هل سبق أن كنتم ضحية فيروسات إعلانية ؟

☐ إطلاقا ☐ أحيانا ☐ غالبا

2- حددوا مصادر هذه الفيروسات :

☐ محامل (اسطوانات وأقراص ...)
☐ بريد إلكتروني (وثائق مرفقة)
☐ أنترنت (جلب الوثائق ...)
☐ أخرى (حددوا) :

3- حددوا إن كان لديكم تطبيق مضادة للفيروسات :

☐ Norton Anti-Virus ☐ F-Prot ☐ TVD ☐ AVP
☐ لا ☐ أخرى (حددوا) :

4- أشيروا إلى دورية تجديد و تطوير تطبيقاتكم المضادة للفيروسات :

☐ أقل من شهر ☐ بين شهر و 3 أشهر ☐ بين 3 شهر و 6 أشهر ☐ بين 6 اشهر و سنة ☐ أكثر من سنة

5- على أي نوع من التجهيزات وضعت مضاد الفيروسات ؟

☐ كل الأجهزة (بما فيها الموزع) المخصصة لتصرفكم الداخلي (محاسبة وشؤون إدارية)

☐ كل الأجهزة (بما فيها الموزع) المخصصة لنشاطكم الرئيسي

6- هل تقومون بمراجعات على التطبيقات و المعطيات الجديدة التي تضعونها على أجهزكم الإعلامية ؟

☐ إطلاقا ☐ أحيانا ☐ غالبا ☐ دائما

7- هل تناول الملحوظات و المنشورات الداخلية للمؤسسة موضوع الفيروسات ؟

☐ إطلاقا ☐ أحيانا ☐ غالبا

السلامة المادية

أ - رقابة الدخول إلى محلات المؤسسة :

أ - هل تستعملون نظام مراقبة للدخول إلى مراكز الإعلامية (مراكز الحاسوب وقاعات التجهيزات الإعلامية ومكاتب إدارات الإعلامية) ؟

☐ نعم ☐ لا

1- الدخول إلى مراكز الإعلامية مرخص إلى :

☐ إطار الإعلامية فقط ☐ كل الأعوان ☐ الأعوان والزائرين

2- ما هو النظام الذي تستعملونه لمراقبة الدخول إلى هذه المراكز ؟

☐ البطاقة ☐ الشفرة ☐ لا شيء ☐ أخرى (حددوا)

3- هل يوجد أثر لكل دخول إلى هذه المراكز ؟

☐ دوريا ☐ يوميا ☐ لا

4- ما هو نظام الرقابة على مراكز الإعلامية الذي تستعملونه خارج أوقات العمل ؟

☐ البطاقة ☐ ترخيص خاص ☐ لا شيء ☐ أخرى (حددوا)

ب - هل تستعملون نظام مراقبة الدخول إلى بقية المحلات (البناءات والمكاتب التابعة للمؤسسة عدى مراكز الإعلامية) ؟

☐ نعم ☐ لا

1- ما هو النظام الذي تستعملونه لمراقبة الدخول إلى هذه المحلات ؟

☐ حراسة ☐ آلي ☐ لا شيء ☐ أخرى (حددوا)

2- ما هي الإجراءات التي تتخذونها لمراقبة دخول الزائرين ؟

☐ حمل الشارة ☐ حضور مرافق داخلي ☐ لا شيء ☐ أخرى (حددوا)

3- هل يوجد أثر عن كل الزائرين ؟

☐ مكتوب (وثيقة تعريف أو الأشخاص الذين تمت زيارتهم) ☐ مسجل على محمل سمعي بصري (شريط فيديو، ...)

☐ لا ☐ أخرى (حددوا)

II - مخاطر الحرائق :

هل لديكم نظام مقاومة ضد الحرائق ؟ ☐ نعم ☐ لا

1- هل يتم احترام منع التدخين في المؤسسة ؟

☐ في مراكز الإعلامية فقط ☐ في كل المحلات ☐ لا

2- هل إن مراكز الإعلامية مجهزة لمجابهة الحرائق ؟

☐ أبواب إيقاف النار ☐ لا ☐ أخرى (حددوا)

3- هل توجد تجهيزات مقاومة ضد الحرائق ؟

☐ مطفأة محمولة ☐ نظام آلي للإطفاء ☐ حفايات حرائق مسلحة ☐ لا ☐ أخرى (حددوا)

4- هل تفحص هذه التجهيزات و تراجع بصفة دورية ؟

☐ إطلاقا ☐ مرة في السنة ☐ مرتان في السنة ☐ أخرى (حددوا)

III - مخاطر المياه :

☐ لا

هل لديكم نظام مقاومة لمجابهة ضرر المياه ؟ ☐ نعم

1- هل توجد كاشفات تسرب المياه في مراكز الإعلامية ؟

☐ في الطوابق العليا لمراكز الإعلامية ☐ في الأسقف الوهمية

☐ لا

☐ أخرى (حددوا)

2- هل يوجد نظام لتصريف المياه من مراكز الإعلامية ؟

☐ أرضية مائلة ☐ ضخ ☐ لا ☐ أخرى (حددوا)

3- هل يتم تفقد نظام التصريف بصفة دورية ؟

☐ إطلاقا ☐ مرة في السنة ☐ مرتان في السنة ☐ أخرى (حددوا)

VI - مخاطر الكهرباء :

☐ لا

☐ نعم

هل لديكم نظام مقاومة لمجابهة مشاكل الكهرباء ؟

1- على أي نوع من التجهيزات وضعت مخففات الصدمات الكهربائية (Onduleurs) ؟

☐ كل الأجهزة (بما فيها الموزع) المخصصة لتصرفكم الداخلي (محاسبة وشؤون إدارية)

☐ كل الأجهزة (بما فيها الموزع) المخصصة لنشاطكم الرئيسي

2- هل توجد ضمن مخففات الصدمات الكهربائية بطاريات تضمن مواصلة العمل ؟

☐ لمدة 10 دقائق ☐ لمدة 20 دقيقة ☐ لا ☐ أخرى (حددوا)

3- هل توجد مع مخففات الصدمات الكهربائية تطبيقات مراقبة و تنبيه ؟

☐ نعم ☐ لا

4- هل يتم صيانة مخففات الصدمات والبطاريات ؟

☐ إطلاقا ☐ مرة في السنة ☐ مرتان في السنة ☐ أخرى (حددوا)

5- هل لديكم تجهيزات نجدة تستخدمونها في حالة حدوث عطب في مستوى اللوحة العامة للضغط الكهربائي (TGBT) ؟

☐ مولد كهربائي ☐ لا ☐ أخرى (حددوا)

V - مخاطر البيئة (الحرارة والرطوبة ...) :

☐ لا

☐ نعم

هل لديكم نظام مقاومة لمجابهة مشاكل البيئة (الحرارة والرطوبة ...) في مراكز الإعلامية ؟

1- هل يوجد نظام تهوية وتكييف في مراكز الإعلامية (مركز الحاسوب ، ...) ؟

☐ نعم ☐ لا

2- هل تباشرون بتسجيل خاصيات الوسط (الحرارة والرطوبة ...) في مراكز الإعلامية ؟

☐ يوميا ☐ أحيانا ☐ إطلاقا

3- هل يتم دوريا صيانة أنظمة التكييف والتهوية ؟

☐ مرة في السنة ☐ مرتان في السنة ☐ لا ☐ أخرى (حددوا)

4- هل يوجد نظام نجدة في صورة تعطب النظام الرئيسي للتكييف والتهوية ؟

☐ نعم ☐ لا

صيانة التطبيقات وحفظ المعطيات

I- إمكانية اشتغال التطبيقات وصيانتها :

1- هل تَحْتَكُمُونَ على شفرة المنشأ للبرمجيات التي تستعملونها في مستوى ؟

☐ تصرفكم الداخلي (المحاسبة ، الشؤون الإدارية ، ...)

☐ نشاطكم الرئيسي

2- من يتكفل بصيانة البرمجيات في حالة حدوث عطب ؟

☐ مؤسسة خدمات

☐ بائع البرمجية

☐ فريق داخلي

3- هل تَمْتَلِكُونَ سجلا لكل تدخلات صيانة برمجياتكم ؟

☐ لا

☐ نعم

II - حفظ المعطيات :

1- هل يتم دوريا حفظ مجموع المعطيات والمعالجات التي تهتم نشاطكم الرئيسي ؟

☐ يوميا

☐ مرة في الشهر على الأقل

☐ بعد إجراء تحويل

☐ إطلاقا

2- من يتولى التصرف في حفظ المعطيات ؟

☐ فريق داخلي : شخص أو مجموعة من إدارة الإعلامية

☐ فريق خارجي : مؤسسة خدمات

3- هل إن إجراءات الحفظ محددة ومكتوبة بشكل واضح ؟

☐ لا

☐ نعم

4- على أي نوع من المحامل يتم الحفظ ؟

☐ قرص مرن ☐ قرص مدمج (CD) ☐ شريط ☐ خرطوشة ☐ قرص صلب ☐ أخرى (حددوا).....

5- هل تقومون بجرد محامل الحفظ ؟

☐ إطلاقا ☐ مرة في الشهر ☐ أخرى (حددوا).....

6- هل تخزن محامل الحفظ في محلات آمنة وبعيدة عن كل المخاطر ؟

☐ لا

☐ نعم

7- توجه محامل الحفظ إلى مراكز خزنها بعد إتمام عملية الحفظ :

☐ إطلاقا ☐ من الغد ☐ بعد أسبوع

☐ مباشرة ☐ أخرى (حددوا).....

8- هل تتأكدون من إن محامل الحفظ يمكن إعادة استخدامها ؟

☐ دائما

☐ مرتان في السنة

☐ مرة في السنة

☐ إطلاقا

مخاطر الاقتحام

1- أشيروا إلى العدد الجملي للهيكل التابعة لمؤسستكم: (يمكن أن يكون الهيكل ، المقر الاجتماعي للمؤسسة أو أي فرع تابع لها)

2- أشيروا إلى عدد الهيكل : - المجهزة بشبكة محلية

- المرتبطة (أي عدد الهيكل التي تتبادل المعلومات فيما بينها عن طريق الإعلامية)

يمكن ترتيب هياكل مؤسستكم حسب الصنف . وتتميز الهيكل من نفس الصنف بالخصائص التالية :

- نفس التشكيلة من التجهيزات والتطبيقات ،
- استغلال معطيات ومعالجات لها نفس درجة الأهمية بالنسبة للمؤسسة .

باشروا بتعريف الجذائذات "أ" و"ب" و"و" أو "ج" لكل صنف من الهيكل

1- الجذائذة "أ" : الدخول إلى الموارد الداخلية من خلال الشبكة المحلية :

يمكن عدم تعميم هذه الورقة بالنسبة للهيكل من نفس الصنف غير المتمتعة بشبكة محلية . ويجب تعميم هذه الورقة عدد المرات ، بمعدل ورقة لكل شبكة محلية إذا كان الهيكل الواحد من نفس الصنف مجهزة بعدد الشبكات المحلية .

2- الجذائذة "ب" : الدخول إلى الموزع المحلي من خلال هيكل خارجي :

يمكن عدم تعميم هذه الورقة بالنسبة للهيكل غير المرتبطة (أي عدم إمكانية تبادل المعلومات مع هيكل أخرى عن طريق الإعلامية) . ويجب تعميم هذه الورقة عدد المرات ، بمعدل ورقة لكل موزع محلي إذا كان الهيكل الواحد من نفس الصنف مجهزة بعدد الموزعات المحلية التي يمكن الدخول إليها من خارج الهيكل .

3- الجذائذة "ج" : الدخول إلى خدمات الأنترنت :

يمكن تعميم هذه الورقة بالنسبة للهيكل من نفس الصنف التي تتمتع بخدمات الأنترنت

الجزء "أ" : النّخول إلى الموارد الداخلية من خلال الشبكة المحلية

الهيكل :
الشبكة المحلية :

1- ما هو نظام الاستغلال للشبكة ؟

Microsoft Windows NT ☐

NetWare Novell ☐

Famille UNIX ☐

OS/400 ☐

أخرى ☐

النسخة :

النسخة :

النسخة :

النسخة :

النسخة :

2- ما هي هندسة شبكتكم المحلية ؟

إيثرنات ETHERNET ☐

DQDB (2 x anneaux) ☐

Toking Ring ☐

FDDI ☐

أخرى (حددوا) ☐

3- ما هو بروتوكول الاتصال الذي تستعملونه ؟

TCP/IP ☐

SNA ☐

IPX/SPX ☐

أخرى (حددوا) ☐

Apple Talk ☐

4- ما هي أداة تراسلكم الداخلي ؟

Microsoft Outlook ☐

لا ☐

Lotus Notes ☐

Outlook Express ☐

أخرى (حددوا) ☐

التعريف بالهوية^① في مستوى الشبكة المحلية :

1- تركز نوعية التعريف بالهوية الذي تستخدمونه على :

مستعمل واحد ☐

مجموعة مستعملين ☐

لا شيء ☐

2- هل يوجد مظهر أو شكل^② لكل مستعمل ؟

نعم ☐

لا ☐

3- يتم تغيير مفاتيح الدخول بصفة دورية كل :

إطلاقا ☐

حدث (إعادة وضع النظام) ☐

شهر ☐

أخرى (حددوا) ☐

4- ما هي أداة التعريف بالهوية التي تستعملونها ؟

أليات ثابتة للتعريف بالهوية (نظام تشغيل) ☐

Security Dynamics ☐

Radius ☐

Save Data ☐

Activcard ☐

أخرى (حددوا) ☐

5- الدخول إلى الشبكة المحلية مرخص :

ساعات العمل فقط ☐

24 ساعة على 24 ساعة ☐

كل الأيام المفتوحة ☐

كل الأيام بما فيها أيام العطل والأعياد ☐

أخرى (حددوا) ☐

① التعريف بالهوية : تحديد وتفقد هويات المستعملين الذين يريدون الدخول إلى الشبكة . ويمكن أن يكون تحديد هوية المستعملين جماعيا في حالة استعمال المجموعة لنفس مفتاح الدخول (مثلا يستعمل كافة أعوان إدارة المحاسبة على سبيل الذكر لا الحصر نفس مفتاح الدخول) . كما يمكن أن يكون تحديد تعريف الهوية لكل شخص على حدة .

② شكل أو مظهر المستعمل : يتحدد حسب المستعمل ، طبيعة الاستعمال للشبكة والخدمات التي تقدمها .

... يتبع :

البجاجة "أ" : الدخول إلى الموارد الداخلية من خلال الشبكة المحلية

الهيكل :
الشبكة المحلية :

☐ لا

☐ نعم

هل تمارسون التشفير؟^①

1- ما هو ألقوريتم التشفير الذي تستعملونه ؟

DES ☐ 3-DES ☐ RSA ☐ أخرى (حددوا)..... ☐

2- على أي معطيات تمارسون التشفير ؟

كلها ☐ مرتبطة بنشاط المؤسسة ☐ تصرف داخلي ☐

☐ لا

☐ نعم

هل تستعملون أدوات كشف الاقتحام؟^②

1- ما هي أدوات كشف الاقتحام التي تستعملونها ؟

AuditWare ☐ Sniffer-Product ☐ Session Wall ☐ Real-Secure ☐

أخرى (حددوا)..... ☐ PC-Firewall ☐ Jummer ☐

2- ما هو دور هذه الأدوات ؟

ثابت : تحليل التدفق ☐ فعال : قطع الارتباط في حالة التنبيه ☐ الاثنان ☐

3- هل لكم أثر للذين دخلوا إلى الشبكة ؟

☐ لا

☐ نعم

① التشفير : تضم الرسائل والوثائق - بواسطة مفتاح ثنائي بين الذات والشفير - ليصبح غموضا غير مفهوم بالنسبة لمستعصي الشبكة - ما عدى الشخص أو الشغل الموجهة إليه الرسائل والوثائق جميعا .

② كشف الاقتحام : هي عملية التفتيش لتدفق المعلومات على الشبكة - لعلايات مريبة كالاستحواذ على اسم المستخدم ومفتاح دحوله .

الجزءة "ب" : الدخول إلى موزع محلي من خلال هيكل خارجي

الهيكل :

الموزع المحلي :

ما هو محمل الاتصال الذي تستعملونه للدخول إلى الموزع ؟

Relay Frame ☐

خط هاتفي RTC ☐

خط مختص LS ☐

Réseau X.25 ☐

.....أخرى (حددوا) ☐

XDSL ☐

ISDN ☐

تجرون تفقد للدخول إلى الموزع :

1- يتم تفقد الدخول إلى الموزع عن طريق :

Firewall d'Axent ☐

Big Fire ☐

FireWall-1 ☐

Routeurs ☐

Firewall de NOKIA ☐

Firewall de CISCO ☐

.....أخرى (حددوا) ☐

Revers Proxy ☐

Proxy ☐

2- يرخص الدخول إلى الموزع

☐ كل الأيام المفتوحة

☐ 24 ساعة على 24 ساعة

☐ كل الأيام بما فيها العطل

☐ ساعات العمل فقط

.....أخرى (حددوا) ☐

☐ ساعات محدودة من اليوم

3- هل يوجد مضاد للفيروسات يسمح بتحليل المعطيات المتبادلة ؟

☐ لا

☐ نعم

... يتبع :

البجاجة "ب" : الدخول إلى موزع محلي من خلال هيكل خارجي

الهيكل :

الموزع المحلي :

التعريف بالهوية :

1- يركز التعريف بالهوية الذي تستعملونه على :

☐ لا

☐ مجموعة أشخاص

☐ شخص واحد

2- هل يوجد مظهر أو شكل لكل مستعمل ؟

☐ لا

☐ نعم

3- يتم تغيير مفاتيح الدخول ، بصفة دورية ، كل :

☐ شهر

☐ أسبوع

☐ إطلاقاً

☐ أخرى (حددوا)

☐ حدث (إعادة وضع نظام)

☐ ثلاثة أشهر

4- ما هي أداة التعريف بالهوية التي تستعملونها ؟

☐ Activcard

☐ Radius

☐ آليات ثابتة للتعريف بالهوية (نظام تشغيل)

☐ أخرى (حددوا)

☐ Save Data

☐ Security Dynamics

☐ لا

☐ نعم

هل تمارسون التشفير ؟

1- ما هو ألقوريتم التشفير الذي تستعملونه ؟

☐ أخرى (حددوا)

☐ RSA

☐ 3-DES

☐ DES

2- ما هي المعطيات التي تقومون بتشفيرها ؟

☐ المرتبطة بالتصرف الداخلي

☐ المرتبطة بنشاط المؤسسة

☐ كلها

الجزء "ج" : الدخول إلى خدمات الإنترنت

الهيكل :

1- ما هي الخدمات التي تستعملونها ؟

☐ Web إبحار وab ☐ نقل المستندات FTP ☐ News ☐ Gopher ☐
☐ Messagerie تراسل ☐ Telnet ☐ أخرى (حددوا)

2- يتم الدخول إلى الخدمات عبر :

☐ أجهزة معزولة : عددها
☐ أجهزة مرتبطة بالشبكة المحلية : عددها

3- ما هي أدوات التراسل التي تستخدمونها ؟

☐ Netscape Communicator ☐ قبل النسخة 4.06 ☐ النسخة 4.06 أو بعدها
☐ Internet Explorer ☐ النسخة 3.01 أو قبلها ☐ بعد النسخة 3.01
☐ Web Notes ☐ النسخة 4.6 أو قبلها ☐ بعد النسخة 4.6
☐ أخرى (حددوا) ☐ النسخة :

4- ما هي أدوات التراسل التي تستخدمونها ؟

☐ Netscape Messenger ☐ Microsoft Outlook ☐ Lotus Notes ☐
☐ Outlook Express ☐ أخرى (حددوا)

☐ لا

☐ نعم

هل تمارسون نظام مراقبة الدخول إلى خدمات الإنترنت ؟

1- ما هي الأدوات التي تستعملونها لمراقبة الدخول إلى خدمات الإنترنت ؟

☐ FireWall-1 ☐ Big-Fire ☐ Firewall d'Axent
☐ Firewall de CISCO ☐ Firewall de NOKIA ☐ Routeurs
☐ Proxy ☐ Revers Proxy ☐ أخرى (حددوا)

2- تؤمن هذه الأدوات :

☐ فرز محتوى الوثائق html لكشف وإلغاء les appels Java المشكوك فيها
☐ فرز محتوى الوثائق html لكشف وإلغاء الرقابات Active X غير المرخصة
☐ فرز Cookies
☐ إدماج مضاد للفيروسات يسمح بتحليل المعطيات والرسائل المتبادلة
☐ متابعة محتوى الرسائل
☐ تحليل صيغ الارتباطات
☐ حماية ضد IP - Spoofing
☐ حماية ضد أدوات Scan et Torjon

3- هل يمكن أن نغلق الدخول إلى خدمات الإنترنت دون تعطيل العمل على الشبكة المحلية ؟

☐ لا

☐ نعم

Evaluation de la Sécurité des Systèmes Informatiques

Identification de l'Organisme

I - Renseignements Généraux :

1. Nom de l'organisme :
2. Nom du responsable :
3. Adresse complète :
4. Téléphone : Fax : E-Mail :

II - Activité :

1. Secteur d'activité :
☐ Administratif ☐ Transport ☐ Santé
☐ Financier ☐ Industrie ☐ Services ☐ Autre (précisez) :
2. Description de l'activité :
3. Effectif global : dont informaticiens

Aspects organisationnels liés à la sécurité

I - Plan de sécurité :

Avez-vous élaboré un Plan de Sécurité ¹ ?

☐ Oui

☐ Non

1. Effectué par :
☐ Equipe interne ☐ Prestataire de service
2. Fait partie d'un schéma directeur :
☐ Oui ☐ Non
3. Le plan de sécurité est validé par :
☐ Direction générale ☐ Direction informatique ☐ Expert externe ☐ CSPPBI
4. Précisez la période prévue pour la mise en œuvre :
Date début : / / Date fin : / /
5. Indiquez le montant total alloué pour la réalisation :mDT

II - Responsable Informatique :

Avez-vous un responsable de la sécurité ?

☐ Oui

☐ Non

1. Ses responsabilités sont-elles clairement définies ? ☐ Oui ☐ Non
2. Est-il informé de tous les incidents relatifs à la sécurité qui surviennent dans l'entreprise ?
☐ Jamais ☐ Quelquefois ☐ Systématiquement

III - Politique de sensibilisation et de formation :

Avez-vous une politique de sensibilisation et de formation sur la sécurité ?

☐ Oui

☐ Non

1. Y a-t-il une politique de sensibilisation aux risques au sein de l'entreprise ?
☐ Aucune ☐ Seulement pour les informaticiens ☐ Pour tout le personnel
2. La politique de sensibilisation aux risques est concrétisée par :
☐ Des instructions orales ☐ Des notes écrites ☐ Autre (précisez):.....
3. Le personnel informatique a-t-il reçu une formation sur la sécurité ?
☐ Jamais ☐ Oui, mais peu ☐ Oui, suffisamment

¹ Si vous avez répondu "Oui" à cette question, et aux autres questions de même style, alors répondez aux questions qui se trouvent dans le cadre qui vient juste après. Sinon passez directement aux questions suivantes.

Les Virus Informatiques

1. Avez-vous déjà été victime de virus informatiques ?

☐ Jamais ☐ Quelquefois ☐ Souvent

2. Précisez la provenance de ces virus :

☐ Supports physiques (disquettes, CD, ...)

☐ Email (fichier rattaché)

☐ Internet (téléchargements de fichiers,...)

☐ Autre (précisez):.....

3. Précisez si vous avez un logiciel anti-virus :

☐ Aucun ☐ TVD ☐ F-prot ☐ Norton Anti virus

☐ AVP ☐ Autre(précisez):.....

4. Indiquez la périodicité de mise à jour de votre anti-virus

☐ Supérieur à 1 an ☐ Entre 1an et 6 mois ☐ Entre 6 et 3 mois ☐ Entre 3 et 1 mois ☐ Inférieur à 1 mois

5. Sur quel type de matériel avez-vous installé l'anti-virus ?

☐ Tous les PC (Serveur inclus) consacré à votre Gestion interne (Comptabilité, Personnel, Bureautique, ...)

☐ Tous les PC (Serveur inclus) consacré à votre Activité principale (Production, ...)

6. Effectuez-vous des vérifications sur les nouvelles applications et données à installer sur vos machines ?

☐ Jamais ☐ Quelque fois ☐ Souvent ☐ Toujours

7. Les notes et publications internes de l'entreprise abordent-elles le sujet des virus (risques, protection,...) ?

☐ Jamais ☐ Quelque fois ☐ Souvent

Les Risques Physiques

I - Contrôle d'accès aux locaux de l'organisme :

A/ Effectuez-vous un contrôle d'accès aux locaux informatiques (Centre de calcul et direction informatique) ?
☐ Oui ☐ Non

1. L'accès aux locaux informatiques est autorisé aux :
☐ Personnel informatique seulement ☐ Tout le personnel ☐ Le personnel et les visiteurs
2. Quel système de contrôle d'accès à ces locaux utilisez-vous ?
☐ Aucun ☐ Par carte ☐ Par code ☐ Autre (précisez):.....
3. Y a-t-il une trace identifiant chaque accès à ces locaux ?
☐ Aucune ☐ Périodique ☐ Journalière
4. En dehors des heures de travail, quel contrôle d'accès aux locaux informatiques effectuez-vous ?
☐ Aucun ☐ Par carte ☐ Par autorisation spéciale ☐ Autre (précisez):.....

B/ Effectuez-vous un contrôle d'accès aux autres locaux ? ☐ Oui ☐ Non

1. Quel système de contrôle d'accès aux locaux utilisez-vous ?
☐ Aucun ☐ Gardiennage ☐ Automatique ☐ Autre (précisez):.....
2. Quelle procédure de contrôle d'accès pour les visiteurs utilisez-vous ?
☐ Aucune ☐ Port de badge ☐ Présence d'un accompagnateur interne ☐ Autre (précisez):.....
3. Y a-t-il une trace sur tous les visiteurs ?
☐ Aucune ☐ Ecrite (Document d'identité, Personne visitée)
☐ Enregistrée sur un support audio-visuel (cassette vidéo, ...) ☐ Autre (précisez):.....

II - Risques des incendies :

Avez-vous un système de lutte contre les incendies ? ☐ Oui ☐ Non

1. L'interdiction de fumer dans l'entreprise est-elle respectée ?
☐ Non ☐ Seulement dans les locaux informatiques ☐ Dans tous les locaux
2. Les locaux informatiques sont-ils équipés pour lutter contre les incendies ?
☐ Non ☐ Porte coupe-feu ☐ Autre (précisez):.....
3. Y a-t-il des installations de lutte contre les incendies ?
☐ Aucune ☐ Installation d'extinction automatique ☐ Installation d'extincteur mobiles
☐ Installation de robinets d'incendie armés ☐ Autre (précisez):.....
4. Ces installations sont-elles périodiquement vérifiées ?
☐ Jamais ☐ 1 fois /an ☐ 2 fois /an ☐ Autre (précisez):.....

République Tunisienne

PREMIER MINISTERE

SECRETARIAT D'ETAT A L'INFORMATIQUE

Evaluation de la Sécurité des Systèmes Informatiques

Identification de l'Organisme

I - Renseignements Généraux :

1. Nom de l'organisme :
2. Nom du responsable :
3. Adresse complète :
4. Téléphone : Fax : E-Mail :

II - Activité :

1. Secteur d'activité :
☐ Administratif ☐ Transport ☐ Santé
☐ Financier ☐ Industrie ☐ Services ☐ Autre (précisez) :
2. Description de l'activité :
3. Effectif global : dont informaticiens

Aspects organisationnels liés à la sécurité

I - Plan de sécurité :

Avez-vous élaboré un Plan de Sécurité ¹ ?

☐ Oui

☐ Non

1. Effectué par :
☐ Equipe interne ☐ Prestataire de service

2. Fait partie d'un schéma directeur :
☐ Oui ☐ Non

3. Le plan de sécurité est validé par :
☐ Direction générale ☐ Direction informatique ☐ Expert externe ☐ CSPPBI

4. Précisez la période prévue pour la mise en œuvre :
Date début : / / Date fin : / /

5. Indiquez le montant total alloué pour la réalisation :mDT

II - Responsable Informatique :

Avez-vous un responsable de la sécurité ?

☐ Oui

☐ Non

1. Ses responsabilités sont-elles clairement définies ? ☐ Oui ☐ Non

2. Est-il informé de tous les incidents relatifs à la sécurité qui surviennent dans l'entreprise ?
☐ Jamais ☐ Quelquefois ☐ Systématiquement

III - Politique de sensibilisation et de formation :

Avez-vous une politique de sensibilisation et de formation sur la sécurité ?

☐ Oui

☐ Non

1. Y a-t-il une politique de sensibilisation aux risques au sein de l'entreprise ?
☐ Aucune ☐ Seulement pour les informaticiens ☐ Pour tout le personnel

2. La politique de sensibilisation aux risques est concrétisée par :
☐ Des instructions orales ☐ Des notes écrites ☐ Autre (précisez):.....

3. Le personnel informatique a-t-il reçu une formation sur la sécurité ?
☐ Jamais ☐ Oui, mais peu ☐ Oui, suffisamment

¹ Si vous avez répondu "Oui" à cette question, et aux autres questions de même style, alors répondez aux questions qui se trouvent dans le cadre qui vient juste après. Sinon passez directement aux questions suivantes.

Les Virus Informatiques

1. Avez-vous déjà été victime de virus informatiques ?

☐ Jamais ☐ Quelquefois ☐ Souvent

2. Précisez la provenance de ces virus :

☐ Supports physiques (disquettes, CD, ...)

☐ Email (fichier rattaché)

☐ Internet (téléchargements de fichiers,...)

☐ Autre (précisez):.....

3. Précisez si vous avez un logiciel anti-virus :

☐ Aucun

☐ TVD

☐ F-prot

☐ Norton Anti virus

☐ AVP

☐ Autre(précisez):.....

4. Indiquez la périodicité de mise à jour de votre anti-virus

☐ Supérieur à 1 an ☐ Entre 1an et 6 mois ☐ Entre 6 et 3 mois ☐ Entre 3 et 1 mois ☐ Inférieur à 1 mois

5. Sur quel type de matériel avez-vous installé l'anti-virus ?

☐ Tous les PC (Serveur inclus) consacré à votre Gestion interne (Comptabilité, Personnel, Bureautique, ...)

☐ Tous les PC (Serveur inclus) consacré à votre Activité principale (Production, ...)

6. Effectuez-vous des vérifications sur les nouvelles applications et données à installer sur vos machines ?

☐ Jamais ☐ Quelque fois ☐ Souvent ☐ Toujours

7. Les notes et publications internes de l'entreprise abordent-elles le sujet des virus (risques, protection,...) ?

☐ Jamais ☐ Quelque fois ☐ Souvent

Les Risques Physiques

I - Contrôle d'accès aux locaux de l'organisme :

A/ Effectuez-vous un contrôle d'accès aux locaux informatiques (Centre de calcul et direction informatique) ?

☐ Oui ☐ Non

1. L'accès aux locaux informatiques est autorisé aux :

☐ Personnel informatique seulement ☐ Tout le personnel ☐ Le personnel et les visiteurs

2. Quel système de contrôle d'accès à ces locaux utilisez-vous ?

☐ Aucun ☐ Par carte ☐ Par code ☐ Autre (précisez):.....

3. Y a-t-il une trace identifiant chaque accès à ces locaux ?

☐ Aucune ☐ Périodique ☐ Journalière

4. En dehors des heures de travail, quel contrôle d'accès aux locaux informatiques effectuez-vous ?

☐ Aucun ☐ Par carte ☐ Par autorisation spéciale ☐ Autre (précisez):.....

B/ Effectuez-vous un contrôle d'accès aux autres locaux ?

☐ Oui ☐ Non

1. Quel système de contrôle d'accès aux locaux utilisez-vous ?

☐ Aucun ☐ Gardiennage ☐ Automatique ☐ Autre (précisez):.....

2. Quelle procédure de contrôle d'accès pour les visiteurs utilisez-vous ?

☐ Aucune ☐ Port de badge ☐ Présence d'un accompagnateur interne ☐ Autre (précisez):.....

3. Y a-t-il une trace sur tous les visiteurs ?

☐ Aucune ☐ Ecrite (Document d'identité, Personne visitée)
☐ Enregistrée sur un support audio-visuel (cassette vidéo, ...) ☐ Autre (précisez):.....

II - Risques des incendies :

Avez-vous un système de lutte contre les incendies ?

☐ Oui ☐ Non

1. L'interdiction de fumer dans l'entreprise est-elle respectée ?

☐ Non ☐ Seulement dans les locaux informatiques ☐ Dans tous les locaux

2. Les locaux informatiques sont-ils équipés pour lutter contre les incendies ?

☐ Non ☐ Porte coupe-feu ☐ Autre (précisez):.....

3. Y a-t-il des installations de lutte contre les incendies ?

☐ Aucune ☐ Installation d'extinction automatique ☐ Installation d'extincteur mobiles
☐ Installation de robinets d'incendie armés ☐ Autre (précisez):.....

4. Ces installations sont-elles périodiquement vérifiées ?

☐ Jamais ☐ 1 fois /an ☐ 2 fois /an ☐ Autre (précisez):.....

III - Risques des eaux :

Avez-vous un système de lutte contre les dégâts des Eaux ?

☐ Oui

☐ Non

1. Existe-t-il des détecteurs de fuite d'eau dans les locaux informatiques ?
☐ Non ☐ Dans les étages supérieurs aux locaux informatiques
☐ Dans le faux planchers ☐ Autre (précisez):.....
2. Existe-t-il un système d'évacuation des eaux dans les locaux informatiques ?
☐ Aucun ☐ Plancher incliné ☐ Système de pompe ☐ Autre (précisez):.....
3. Ce système d'évacuation est-il périodiquement testé ?
☐ Jamais ☐ 1 fois /an ☐ 2 fois /an ☐ Autre (précisez):.....

IV - Risques électriques :

Avez-vous un système de lutte contre les problèmes d'électricité ?

☐ Oui

☐ Non

1. Sur quel type de matériel avez-vous installé des onduleurs ?
☐ Tous les PC (Serveur inclus) consacré à votre Gestion interne (Comptabilité, Personnel, Bureautique, ...)
☐ Tous les PC (Serveur inclus) consacré à votre Activité principale (Production, ...)
2. Y a-t-il des batteries dans ces onduleurs garantissant une autonomie :
☐ Non ☐ de 10 mn ☐ de 20 mn ☐ Autre (précisez):.....
3. Y a-t-il avec les onduleurs des logiciels de surveillance et d'alarmes ?
☐ Oui ☐ Non
4. La maintenance des onduleurs et des batteries se fait :
☐ Jamais ☐ 1 fois /an ☐ 2 fois /an ☐ Autre (précisez):.....
5. En cas de problème au niveau du Tableau Général de Basse Tension avez-vous une installation de secours ?
☐ Aucune ☐ Un groupe électrogène ☐ Autre (précisez):.....

V - Risques d'environnement (Chaleur, Humidité, ...):

Avez-vous un système de lutte contre les problèmes d'environnement (Chaleur, humidité,...) dans les locaux informatiques ?

☐ Oui

☐ Non

1. Y a-t-il un système de climatisation dans les locaux informatiques (centre de calcul) ?
☐ Oui ☐ Non
2. Procédez-vous à l'enregistrement des caractéristiques de l'ambiance dans les locaux informatiques (température, Humidité, ...) ?
☐ Jamais ☐ Quelques fois ☐ Tous les jours
3. Y a-t-il une maintenance périodique du système de climatisation ?
☐ Non ☐ 1 fois /an ☐ 2 fois /an ☐ Autre (précisez):.....
4. Existe-t-il un système de secours en cas de panne du système principal ?
☐ Oui ☐ Non

Fiabilité et maintenance des logiciels et Sauvegarde des données

I- Fiabilité et maintenance des logiciels :

1. Disposez-vous des codes sources des applicatifs que vous exploitez au niveau de votre :
 - ☐ Gestion interne (Comptabilité, Personnel, Bureautique, ...)
 - ☐ Activité principale
2. En cas de problèmes, qui se charge de la maintenance des applicatifs
 - ☐ Une équipe interne
 - ☐ Le fournisseur de l'applicatif
 - ☐ Autre prestataire de services
3. Possédez-vous un journal sur toutes les interventions de maintenance de vos applicatifs ?
 - ☐ Oui
 - ☐ Non

II- Elaboration des Sauvegardes :

1. L'ensemble des données et des traitements qui concernent votre activité principale sont-ils périodiquement sauvegardés ?
 - ☐ Jamais
 - ☐ Après une modification
 - ☐ au minimum 1 fois / mois
 - ☐ Tous les jours
2. Qui se charge de la gestion des sauvegardes ?
 - ☐ Une entité interne : Une ou plusieurs personnes de la direction informatique
 - ☐ Une entité externe : un prestataire de services
3. Les procédures de sauvegarde sont-elles clairement définies et écrites ?
 - ☐ Oui
 - ☐ Non
4. Les sauvegardes sont effectuées sur quel type de support ?
 - ☐ Disquette
 - ☐ CD
 - ☐ Cassettes
 - ☐ Cartouches
 - ☐ Disque dur
 - ☐ Autre (précisez):.....
5. Effectue-t-on un inventaire physique des supports de sauvegarde ?
 - ☐ Jamais
 - ☐ 1 fois /mois
 - ☐ Autre (précisez):.....
6. Les sauvegardes sont-elles stockées dans des locaux sécurisés et éloignés de tout risque ?
 - ☐ Oui
 - ☐ Non
7. Une fois prêtes, les sauvegardes sont envoyées à leur lieu de stockage :
 - ☐ Jamais
 - ☐ Immédiatement
 - ☐ Le lendemain
 - ☐ Après une semaine
 - ☐ Autre (précisez):.....
8. Contrôlez-vous qu'une reprise est effectivement possible à partir de ces sauvegardes ?
 - ☐ Jamais
 - ☐ 1 fois./an
 - ☐ 2 fois /an
 - ☐ Toujours

Risques des Intrusions logiques

1. Indiquez le nombre total de sites appartenant à votre organisme :

(Un site peut être le siège de l'organisme, tout autre bâtiment géographiquement distant et/ou toute représentation régionale)

--	--	--

2. Indiquez le nombre de sites - Equipés d'un réseau local :

- Interconnectés :

(c'est à dire le nombre de sites ayant entre eux des échanges informatisés d'informations)

Les sites de votre organisme peuvent être classés en Types. Les sites d'un même Type sont caractérisés par :

- * La même plate-forme technique : c'est à dire disposant de la même configuration matérielle et logicielle,
- * L'exploitation de données et d'applicatifs semblables ou ayant le même degré d'importance par rapport à l'activité de l'organisme.

Pour chaque Type de sites, procédez au remplissage des fiches A, B et/ou C

1- Fiche A = Accès aux ressources internes depuis le réseau local

Dans un Type donné, les sites peuvent ne pas avoir de réseau local, dans ce cas il n'y a pas lieu de remplir cette fiche. Comme ils peuvent être équipés chacun de plusieurs réseaux locaux, dans ce cas cette fiche sera remplie plusieurs fois (une pour chaque réseau local).

2- Fiche B = Accès à un serveur local depuis un site externe

Dans un Type donné, les sites peuvent ne pas être accessibles de l'extérieur (c'est à dire qu'ils n'effectuent pas d'échanges informatisés d'information avec d'autres sites) dans ce cas, il n'y a pas lieu de remplir cette fiche. Par contre, ils peuvent disposer chacun de plusieurs serveurs locaux accessibles de l'extérieur (sachant qu'un serveur local peut être indépendant ou relié à un réseau local), dans ce cas cette fiche sera remplie plusieurs fois (une pour chaque serveur local)

3- Fiche C = Accès aux services Internet

Cette fiche sera remplie seulement dans le cas où les sites d'un Type donné accèdent aux services Internet.

Fiche A : Accès aux ressources internes depuis le réseau local

Site :

Réseau Local :

1. Quel est votre système d'exploitation réseau ?

☐ Microsoft Windows NT

Version :

☐ NetWare (Novell)

Version :

☐ Famille UNIX (AIX,...)

Produit :

Version :

☐ OS/400

Version :

☐ Autre :

Version :

2. Quelle est l'architecture de votre réseau local ?

☐ Ethernet

☐ Token Ring

☐ FDDI

☐ DQDB (2 x anneaux)

☐ Autre (précisez):.....

3. Quel protocole de communication utilisez-vous ?

☐ TCP/IP

☐ IPX/SPX

☐ Apple Talk

☐ SNA

☐ Autre (précisez):.....

4. Quel est votre Outil de messagerie interne ?

☐ Microsoft Outlook

☐ Lotus Notes

☐ Outlook Express

☐ Aucun

☐ Autre (précisez):.....

Authentification ⁽¹⁾ au niveau du réseau local

1. Quel type d'authentification effectuez-vous ?

☐ par utilisateur

☐ par groupe d'utilisateurs

☐ Aucun

2. Y a-t-il un profil ⁽²⁾ pour chaque utilisateur ?

☐ Oui

☐ Non

3. Le changement des mots de passe se fait de manière périodique par :

☐ Semaine

☐ Trimestre

☐ Événement (Réinstallation du système, ...)

☐ Mois

☐ Jamais

☐ Autre (précisez):.....

4. Quels outils d'authentification utilisez-vous ?

☐ Mécanismes d'authentification standard (intégrés dans l'OS)

☐ RADIUS

☐ Activcard

☐ Security Dynamics

☐ Save Data

☐ Autre (précisez):.....

5. L'accès au réseau local est autorisé :

☐ 24h/24h

☐ Tous les jours ouvrables

☐ Heures de travail seulement

☐ Tous les jours, Week-End et jours fériés inclus

☐ Autre (précisez):.....

1 Authentification : Identification et vérification de l'identité des utilisateurs qui veulent accéder à un réseau. L'authentification peut se faire pour "Un groupe d'utilisateurs" dans ce cas tous les utilisateurs du groupe ont le même mot de passe pour accéder au réseau (Exemple : les membres de la direction du personnel ont le même mot de passe). Comme elle peut se faire par utilisateur, dans ce cas chaque utilisateur est identifié par son propre mot de passe.

2 Profil utilisateur : C'est la possibilité de définir pour un utilisateur donné des droits d'accès à un ensemble restreint de services parmi tous les services disponibles sur le réseau.

Suite Fiche A : Accès aux ressources internes depuis le réseau local

Site :

Réseau Local :

Procédez-vous au cryptage ⁽¹⁾ ?

☐ Oui

☐ Non

1. Quel algorithme de cryptage utilisez-vous

☐ DES

☐ 3-DES

☐ RSA

☐ Autre (précisez) :

2. Sur quelle données effectuez-vous le cryptage

☐ Toute

☐ Liées à l'activité de l'organisme

☐ Gestion Interne

Utilisez-vous des outils de Détection d'Intrusions ⁽²⁾ (Sniffeur) ?

☐ Oui

☐ Non

1. Quel outils de détection d'intrusion utilisez-vous ?

☐ Real-Secure

☐ Session-Wall

☐ Sniffer-Product

☐ AuditWare

☐ Jummer

☐ PC-FireWall

☐ Autre (précisez) :

2. Quel est le rôle de ces outils ?

☐ Passif = Analyse le flux

☐ Actif = Coupe la connexion en cas d'alerte

☐ Les deux

3. Avez-vous une trace logique des accès au réseau ?

☐ Oui

☐ Non

1 Cryptage : c'est le fait de chiffrer ou de coder le contenu d'un message ou d'un fichier pour le rendre incompréhensible par une autre personne à part celle à laquelle il est destiné. En effet, cette dernière est capable via un code de déchiffrer le message ou le fichier.

2 Détection d'intrusions :

Intrusion : C'est le fait d'écouter, en interne ou en externe, le flux de données circulant sur un réseau.

Sniffeur : C'est un programme installé sur une machine pour écouter le flux sur le réseau et collecter tous les (Login/Password) qui y transitent

Fiche B : Accès à un serveur local depuis un site externe

Site :

Serveur local :

Quel support de communication utilisez-vous pour accéder au serveur ?

☐ Réseau X.25

☐ LS

☐ RTC

☐ Frame Relay

☐ ISDN

☐ XDSL

☐ Autre (précisez) :

Vous effectuez un contrôle d'accès au serveur

1. Le Contrôle d'accès au serveur est assuré par :

☐ FireWall-1

☐ Big Fire

☐ Firewall d'Axent

☐ Firewall de CISCO

☐ Firewall de NOKIA

☐ Routeurs

☐ Proxy

☐ Revers Proxy

☐ Autre (précisez) :

2. L'accès est autorisé

☐ 24h/24h

☐ Tous les jours ouvrables

☐ Heures de travail seulement

☐ Tous les jours, Week-End et jours fériés inclus

☐ Des heures bien déterminés de la journée

☐ Autre : (Précisez) :

3. Y a-t-il une Intégration d'un anti-virus permettant l'analyse des données transférées

☐ Oui

☐ Non

Authentification

1. Quel type d'authentification effectuez-vous

☐ par utilisateur

☐ par groupe d'utilisateurs

☐ Aucun

2. Y a-t-il un profil pour chaque utilisateur

☐ Oui

☐ Non

3. Le changement des mots de passe se fait de manière périodique par

☐ Semaine

☐ Trimestre

☐ Evènement (Réinstallation du système, ...)

☐ Mois

☐ Jamais

☐ Autre : (Précisez) :

4. Quels outils d'authentification utilisez-vous

☐ Mécanismes d'authentification standard (intégrés dans l'OS)

☐ RADIUS

☐ Activcard

☐ Security Dynamics

☐ Save Data

☐ Autre : (Précisez) :

Procédez-vous au cryptage ?

☐ Oui

☐ Non

1. Quel algorithme de cryptage utilisez-vous

☐ DES

☐ 3-DES

☐ RSA

☐ Autre :

2. Sur quelle données effectuez-vous le cryptage

☐ Toute

☐ Liées à l'activité de l'organisme

☐ Gestion Interne

Fiche C : Accès aux services Internet

Site :

1. Quels sont les services que vous utilisez ?

- ☐ Navigation Web
- ☐ FTP
- ☐ News
- ☐ Gopher
- ☐ Messagerie
- ☐ Telnet
- ☐ Autre : (Précisez)

2. L'accès à ces services se fait via des

- ☐ Postes isolés
 - ☐ Postes connectés au réseau local
- Nombre :

- Nombre :

3. Quels outils de navigation utilisez-vous ?

- ☐ Netscape Communicator
- ☐ Avant la version 4.06
- ☐ Version 4.06 ou postérieure
- ☐ Internet Explorer
- ☐ Version 3.01 ou antérieure
- ☐ Après la version 3.01
- ☐ Web Notes
- ☐ Version 4.6 ou antérieure
- ☐ Après la version 4.6
- ☐ Autre : (Précisez)
- ☐ Version =

4. Quels outils de messagerie utilisez-vous ?

- ☐ Netscape Messenger
- ☐ Microsoft Outlook
- ☐ Lotus Notes
- ☐ Outlook Express
- ☐ Autre : (Précisez)

Effectuez-vous un contrôle d'accès aux services Internet ?

☐ Oui

☐ Non

1. Quels outils de contrôle d'accès aux services Internet utilisez-vous ?

- ☐ FireWall-1
- ☐ Big Fire
- ☐ Firewall d'Axent
- ☐ Firewall de CISCO
- ☐ Firewall de NOKIA
- ☐ Routeurs
- ☐ Proxy
- ☐ Revers Proxy
- ☐ Autre : (Précisez)

2. Ces outils assurent

- ☐ Filtrage dans le contenu des documents HTML pour détecter et éliminer les applets Java suspectes
- ☐ Filtrage dans le contenu des documents HTML pour détecter et éliminer des contrôles Active X non certifiés
- ☐ Filtrage des Cookies
- ☐ Intégration d'un anti-virus permettant l'analyse des données et les messages transférées
- ☐ Contrôle du contenu des messages
- ☐ Analyse des contextes des connexions
- ☐ Protection contre l'IP-Spoofing
- ☐ Protection contre les Outils de Scan et Torjon

3. Pour les applications et les données importantes, a-t-on la possibilité de fermer l'accès Internet sans bloquer les connexions internes

☐ Oui

☐ Non