الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ عامة في السلامة الرقمية

الفـئة المسـتهـدَفـة

العاملون في المجال الصحي

كُتَيّب المدرّب

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

تمهـــيد

السلامــة الرقمية لــم تَعُد خيارًا، بــل أصبحت ركيزة أساسية لضمان أمن المعلومات الطبية، وحمايــة المرضــى والعامليــن فــي المجال الصحي من التهديــدات السيبرانيــة المتزايدة تعقيدًا وشراســةً.

وقد تــم تصميم هــذا الكُتَيِّب ليكون مرشــدًا عمليًّا لأولئــك الذين يُوجدون فــي الخطوط الأماميــة للدفــاع عن حيــاة المرضــى، ليس فقط في العالــم المادي، بل وفــي الفضاء السيبراني الذي أصبح ســاحة رئيســية للحفاظ على خصوصية واســتمرارية الخدمات الطبية.

يهدف هذا الكُتَيّب لرَفْــع وَعْي العاملين في المجــال الصحي بمبــادئ السلامــة الرقمية، وتعزيــز قُدراتهــم علــى حمايــة المعلومات الطبية وبيانات المرضــى في بيئة عمل تتزايد فيها التهديــدات السيبرانية، وتتطــوَّر أدواتها باســتمرار. ويُســلِّط الضوء علــى أبرز المخاطر الرقمية في بيئة العمــل الصحية من هجمات التصيُّد المُوجَّهة بدقة إلى برمجيات التجسُّــس المتقدّمة.

يتضمّن أفضل الممارسات والإجراءات الوقائية لحماية الأجهزة والحســابات الرسمية، وضمان سلامة الاتصالات الطبية، والاستجابة الفعَّالة والمنظّمة للحوادث السيبرانية.

وتُعدّ هذه الجهود جزءًا مــن المبادرة الوطنية للسلامــة الرقميــة التــي تُنظّمهــا الوكالة الوطنيــة للأمــن السيبراني، لبنــاء بيئة رقمية آمِنَــة لجميع فئــات المجتمع.

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative

تعريف المبادرة

مجموعة من فعاليات التوعية في مجال السلامة الرقمية والأمن السيبراني؛ تستهدف المجتمع المحلي على اختلاف الشرائح العُمرية والاجتماعية والقطاعات المهنية.

تعمل المبادرة على نَشْر الوعي بالسلامة الرقمية والاستخدام الآمِن لشبكة الإنترنت والتطبيقات التكنولوجية المختلفة، وتوضيح المخاطر المحتمَلة؛ وذلك بهدف بناء مجتمع آمِن سيبرانيًّا ومُتمكِّن تكنولوجيًّا.

الشرائح المُستهدَفة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها على الفئات التالية:

01 السنة الأولى

كبار القَدْر

المرأة والأسرة

العمالة الوافدة

مؤسسات المجتمع المدني

القطاع المالي والمصرفي

طلبة الجامعات

ذوو الاحتياجات الخاصة

02 السنة الثانية

الدبلوماسيون

الإعلاميون

الرياضيون

المؤسسات العقابية والنيابة والمؤسسات الإصلاحية

العاملون في المجال الصحي

المرأة (العنف الرقمي ضد المرأة)

الجمهور العام

03 السنة الثالثة

العاملون في قطاع الطاقة

العاملون في وزارتي الدفاع والداخلية

ذوو الاحتياجات الخاصة

اليافعون والشباب

الجمهور العام

العاملون في قطاع التعليم

المحور الأول

الوكالة الوطنية للأمن السيبراني وحمـايـة المجتـــمع الرقمـــي

التأسيس والأهداف

التأسيس

تأسَّست الوكالة الوطنية للأمن السيبراني بمُوجب المرسوم الأميري رقم (1) لعام 2021م، كمرجعيَّة وطنية لحماية الفضاء السيبراني؛ بهدف تعزيز الأمن السيبراني للدولة، وضمان حماية الأصول الرقمية والبِنْية التحتية الحيوية من التهديدات السيبرانية المتزايدة.

الأهداف

تعزيز الأمن السيبراني

تطوير سياسات مُتقدّمة لضمان حماية الأنظمة الرقمية، وتطبيق إجراءات وقائية شاملة للكشف عن التهديدات السيبرانية، ومعالجتها

رَفْع مستوى الوعي

تنظيم برامج تدريبية وحملات توعية تهدف إلى تثقيف الأفراد والمؤسسات حول أهمية الأمن السيبراني، وكيفية التصدّي للهجمات السيبرانية

بناء القدرات الوطنية

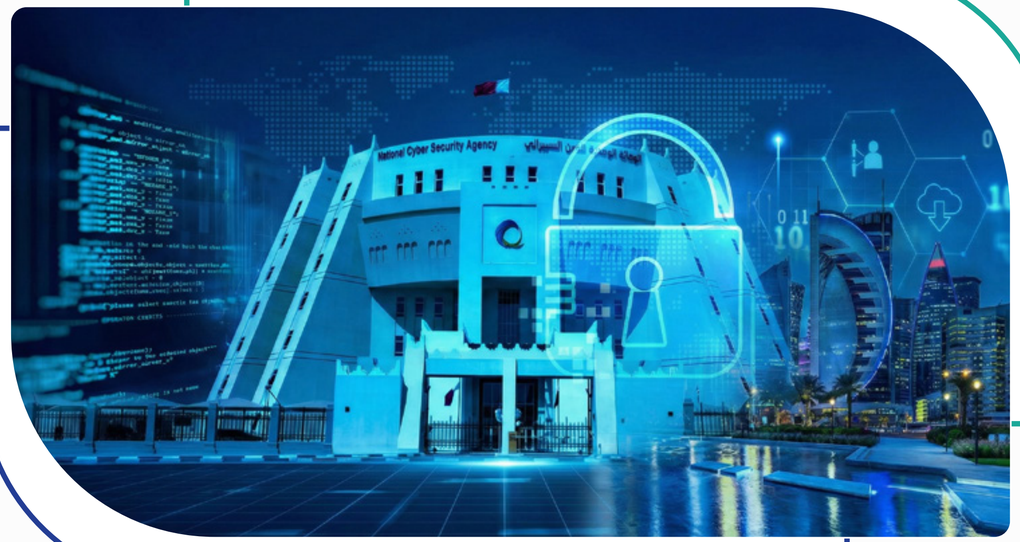
تدريب الكوادر الوطنية على أحدث تقنيات الأمن السيبراني، ودعم الأبحاث والدراسات التي تُعزِّز من قدرة الدولة على التصدّي للتحديات السيبرانية

التعاون الدولي

إقامة شراكات مع المنظمات الدولية، وتبادل الخبرات مع الدُّوَل الرائدة في مجال الأمن السيبراني؛ لمكافحة الجرائم السيبرانية، وتعزيز الحماية السيبرانية

الرؤية والاختصاصات

الرؤية الإستراتيجية



- بلـوغ فضـاء سـيبراني آمِـن يدعـم التنميـة الاجتماعيـة والاقتصاديـة
- تمكيـن اقتصـاد المعرفـة عَبْـر تعزيـز الثقـة فـي الخدمـات الرقميـة

الاختصاصات

01

إعداد وتنفيذ الإستراتيجية الوطنية للأمن السيبراني

02

رَصْد التهديدات السيبرانية والاستجابة للحوادث عبر فِرَق متخصصة

03

وضع السياسات والمعايير الفنية والتنظيمية لحماية البنية التحتية الرقمية

04

تنسيق الجهود الوطنية بين الجهات الحكومية والخاصة في مجال الأمن السيبراني

05

رَفْع الوعي المجتمعي حول الأمن السيبراني من خلال حملات وبرامج تدريبية

06

تمثيل الدولة دوليًّا في المحافل والاتفاقيات المتعلّقة بالأمن السيبراني

07

تطوير خبرات الكوادر الوطنية عبر التدريب والشهادات المهنية في المجال

التكامل في التعامل مع الجرائم الإلكترونية

تتكامل الأدوار بين الوكالة الوطنية للأمن السيبراني ووزارة الداخلية في حماية الفضاء الرقمي.

دور الوكالة الوطنية للأمن السيبراني

1. إطلاق المبادرات الوطنية للسلامة الرقمية.
2. إعداد السياسات والمعايير والإجراءات الوقائية.
3. تنفيذ برامج التوعية والتثقيف المجتمعي.
4. تقديم الدعم الفني والتقني للقطاعات المختلفة.
5. رَصد ومتابعة التهديدات الرقمية على المستوى الوطني.

دور وزارة الداخلية

1. التحقيق في الجرائم الإلكترونية وضبط مرتكبيها.
2. جَمْع الأدلة الرقمية وفق الأُطُر القانونية.
3. حماية المجتمع من الأنشطة الإجرامية عبر الإنترنت.
4. التنسيق مع الإنتربول والجهات الأمنية الدولية عند الحاجة.
5. تطبيق العقوبات وفق القوانين ذات الصلة بالجرائم الإلكترونية.

وزارة الداخلية
Ministry of Interior
State of Qatar • دولة قطر

المحور الثاني

التهديدات السيبرانية الشائعة في المجـــال الصحـــي

التصيد الاحتيالي

الهجوم الأكثر شيوعًا في القطاع الصحي؛ حيث يرسل المهاجمون رسائل بريد إلكتروني أو رسائل نصية مزيفة تتظاهر بأنها من الإدارة الطبية أو موردي الأدوية لطلب بيانات تسجيل الدخول أو النقر على روابط خبيثة.

مؤشرات التصيد

- عناوين بريد إلكتروني غريبة مثل admin-support@hospital-security.co
- روابط مختصرة مشبوهة أو أخطاء إملائية
- طلب معلومات عاجلة دون إجراءات التحقّق المعتادة

التصيد المخصَّص للعاملين في المجال الصحي

يســتخدم المهاجمون بيانات مســربة مسبقًا من المستشفيات لإرسال رســائل مخصَّصة تحمل أسماء الأطباء والمرضى الحقيقيين

هذه الرســائل تُظهر شــعار المستشفى الحقيقي، وتســتخدم عناوين بريد تبدو رســمية، مما يجعلها أكثر خطرًا من التصيد العام بنســبة 300%

تشــهد المستشــفيات حملات مُكثَّفة تستمر أســابيع؛ حيث يُرســل المهاجمون 5000 رسالة يوميًّا لنفس المستشــفى باختلافات طفيفة حتــى تنجح واحدة

فــي 2024، أبلغت 73% من المستشــفيات عن حــملات تصيُّد ناجحة أدَّت لحــدوث اختراق. وكان الضحيــة الأولى دائمًا مُوظّف اســتقبال، أو ممرضًا، وليس قســم IT

سؤال تفاعلي

اذكر مثالًا على رسالة بريد إلكتروني قد تكون محاولــة تصيُّد احتيالي لشــبكة مستشــفى.

البرمجيات الخبيثة

- برمجيات ضارَّة تُصيب أجهزة المستشفيات عبر المُرفَقات، ومُحرّكات USB، أو مواقع ويب مُصابة، مما يسمح بالتجسُّس، وسرقة البيانات، أو تعطيل الخدمات الطبية.
- قد يَحْدُث الهجوم عند إرسال رسائل تطلب "تحديث بيانات المرضى"، أو تفعيل "حساب نظام السجلات"، وبمجرد الضغط على المرفقات تُصيب البرمجيات الخبيثة الأنظمة الرقمية EMR أو السجلات الطبية الإلكترونية.

الأضـــرار المتوقَّـعة

- إيقاف أنظمة السجلات الطبية (EMR/EHR)
- تعطيل أجهزة التصوير الطبي (MRI/CT)
- تعطيل أنظمة الصيدليات وتوزيع الأدوية

إحصـائيـة

في حادثة Universal Health Services 2020، أدَّى توقُّف أنظمـة EMR إلـى **إلغاء 45 عمليـة** جراحية طارئة **ووفاة 5 مرضى** بسـبب تأخير الأدوية الحيوية.

برمجيات تستهدف المجال الصحي

- **تـورجـانـات**: تَسـرق بـيانات المـرضى وتُرسلـها للمهاجمـين.
- **Keyloggers**: تُسجّل كلمات المرور لأنظمة السجـلات الطبـية.
- **Rootkits**: تُخفي وجودها، وتُمَكِّن المهاجِم من التَّحكُّم الكامل.

أعـراض الإصـابـة

- تباطؤ مفاجئ في أجهزة الحواسيب الطبية
- ظهور نوافذ غير متوقَّعة أو ملفات جديدة
- زيادة استهلاك المعالج أو الذاكرة بشكل غير طبيعي

إحصـائيـة

فـي 2024 سُـرِقَت بيانات **89 مليـون** مريض أمريكي من خلال برمجية خبيثـة، بقيمة تصل إلى **$1,000** لكل سـجل في "الـدارك ويب". هـذه البرمجيات لا تسـرق فقـط، بـل تُغَيِّـر التشـخيصات والجرعات الطبيـة أيضًا

سؤال تفاعلي

ما الأضرار المحتملة لإصابة أنظمة السجلات الطبية ببرمجيات خبيثة؟

سرقة البيانات

سـرقة البيانـات الطبيـة تَسـتهدف سـجلات المرضـى الحسَّاسـة (تشـخيصات، علاج، بيانـات ماليـة) لبيعهـا فـي شـبكات الويـب المظلـم، أو بهـدف ابتـزاز المرضـى.

البيانات الأكثر قيمة

1. أرقام التأمين الصحي
2. وثائق الحالة الطبية
3. وصفات الأدوية النفسية والمزمنة
4. نتائج الفحوص الوراثية والجينية
5. سجلات العلاج النفسي والإدمان

هجمات حَجْب الخدمة الموزّعة

هجمات تُغرق خوادم المستشفيات بحركة مرور مُزيَّفة؛ مما يُوقِف مواقع الحجز، بوّابات المرضى، وأنظمة الطوارئ الرقمية.

التأثير الطبي

1. إيقاف نظام حجز المواعيد الإلكتروني
2. تعطُّل بوابة المريض لعرض النتائج
3. شلّ أنظمة الطوارئ لاستدعاء الإسعاف

أهداف شائعة

1. مواقع المستشفيات الرئيسية
2. تطبيقات المرضى المتنقّلة
3. أنظمة التواصل بين المستشفيات

تأثير هجمات حَجْب الخدمة

- مَنْع المرضى من الوصول إلى نتائج العلاج والتقارير الطبية
- عدم التمكّن من الوصول إلى السجلات الطبية/ التاريخ الطبي للمرضى
- تعطُّل الأنظمة الفنية والطبية في المستشفيات
- إجبار المرضى المستفيدين من الاستشارات الطبية على الذهاب إلى المستشفى بدلًا من المتابعة الإلكترونية
- تعطُّل أنظمة الإسعاف؛ مما يُؤخّر الاستجابة للحوادث بنسبة 40%

إحصائية

في حادثة Clop ransomware 2023، أدَّت هجمات حجب الخدمة الموزعة إلى إلغاء 3,200 موعد علاج أورام، ووفاة مريضين؛ بسبب تأخُّر الإسعاف لمدة ساعتين.

الهجمات المُركَّبة

يلجــأ المهاجمون في بعض الجرائم للجمــع بين هجمات حجب الخدمة الموزعــة وبرمجيات الفدية في هجــوم واحد؛ يبدأ بإِلْهَــاء فريق الدعم التقني، ثــم زَرْع برمجية ضارَّة لســرقة وحجب البيانات، حتى يتم دفــع مبلغ مالي.

مثــال:

تســبب هجــوم مُركَّب على **17 مستشــفى** فــي بريطانيا عــام **2024** لمدة **72 ســاعة** متتالية، في خســائر تُقــدَّر بـ **£23 مليونًــا**، وإلغــاء **28,000** موعد طبي.

هجمات التزييف العميق

تَستخدم هجمات التزييف العميق الذكاء الاصطناعي لإنشاء فيديوهات أو مكالمات صوتية مُزيَّفة لطبيب، أو مدير مستشفى؛ لطلب بيانات أو معاملات مالية من الضحايا.

التصيد الصوتي الطبي المتقدّم

يَستخدم المهاجمون تسجيلات صوتية سابقة لأطباء المستشفى من اجتماعات زووم Zoom أو مكالمات داخلية لإنشاء مكالمات صوتية واقعية تطلب "بيانات مريض طارئ للنقل"، أو "تحديث حسابات فوري"؛ حيث يتفاعل الصوت مع أسئلة الموظف بشكل طبيعي تمامًا، مما يخدع حتى الموظفين المدربين.

التزييف البصري للوثائق الطبية

يُستخدم التزييف العميق في إعداد تقارير طبية مُزيَّفة بأسماء وتواريخ مرضى حقيقيين تَحْمل توقيعًا إلكترونيًّا لطبيب معروف، تُستخدَم لوَصْف أدوية باهظة الثمن لمطالبات تأمين احتيالية، أو نتائج تحاليل مخبرية تُظْهِر أمراضًا وهمية للحصول على تعويضات إعاقة.

التزييف العميق للوثائق الطبية

التزييــف العميــق للوثائق يَســتخدم الــذكاء الاصطناعي لإنشــاء تقارير طبية، وصفــات علاجيــة، أو نتائج فحــوص مُزيّفة تبدو أصليــة تمامًا للخــداع أو الابتزاز.

الاستخدام في الاحتيال الطبي المُنظَّم

يُنشــئ المجرمون وصفــات طبية مُزيَّفة بأســماء وتوقيعــات أطبــاء حقيقييــن؛ لتوزيعهــا فــي الصيدليات، أو تقارير أشــعة تُظْهِر إصابات خطيرة وَهْمية للحصول على تعويضــات مادية.

الابتزاز طويل الأمد للمرضى

يُســتخدم التقــرير الطبي المُزيَّــف بالكامل لابتزاز المريــض بـ"نتائــج فحوص ســرية"؛ تُظهــر أمراضًا مُخجلــة أو غير صحيحة، ممــا يُجبره على دَفْع مبالغ شــهرية لمنع "النشــر"، أو يُبــاع كـ"ملف طبــي كامل" في الإنترنــت المظلم للاســتخدام في جرائم الهويــة الطبية.

الوثائــق المُزيَّفــة الشــائعــة

تقــارير MRI/CT مزيفــة

وصفات طبية غير حقيقية

نتائج تحاليل مخبرية مُزوَّرة

تفريغ طبــي كامل مُزيَّف

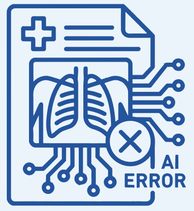
سؤال تفاعلي

ما الفرق بين هجمات التزييف العميق الصوتية والبصرية في المجال الطبي؟

تسميم البيانات الطبية

يُسمَّى أيضًا تسميم البيانات (Data Pioisoning)، ويحدث عندما يُدْخِل المهاجمون بيانات خطأ في نماذج الذكاء الاصطناعي الطبي، ممَّا يُؤدِّي لتشخيصات غير صحيحة أو جرعات أدوية خطيرة.

التلاعب بالتشخيصات الآلية



يُدْخِل المهاجمون صور أشعة مُزيَّفة في تدريب خوارزميات الذكاء الاصطناعي للأشعة، فتُخْرِج تقارير خطأ لآلاف المرضى دون أن يكتشف الطبيب البشري الخطأ المخفي.

الجرعات الدوائية الفتاكة

يتم تسميم قواعد بيانات الجرعات بإضافة حالات وهمية تُظهر أن "مضاعفة جرعة المورفين آمنة لكبار القَدْر"، أو أن "تقليل جرعة الأنسولين لمرضى السكري الشديد لا ضرر فيه"؛ مما يؤدّي لتناول جرعات زائدة مميتة أو نقص حيوي يُصِيب المريض بالغيبوبة.

الأهداف الطبية

- تسميم خوارزميات التشخيص بالأشعة
- تغيير توصيات الجرعات الآلية
- إفساد قواعد بيانات التنبؤ بالأوبئة

التـأثيــر

تشخيصات غير صحيحة بنسبة تصل إلى 30%

جرعـات زائـدة أو نـاقصـة للأدويـة

فقـدان الثقـة فـي أنظمـة الـذكاء الاصطناعـي الطبيـة

التلاعُب بالبيانات الطبية

تُتِيح أنظمــة الذكــاء الاصطناعي الطبية التلاعب ببيانات المرضى؛ ما يُؤثِّر سلبًا على دقة قرارات التشخيص.

مثــال:

عندمــا يُصْدِر نظــام الذكاء الاصطناعي تقريرًا طبيًّا بــنسبة **"95% ثقة"** يُفيد بعــدم وجود خطر؛ يميل الأطبــاء لقبوله دون تدقيق بشــري، خاصةً فــي أوقات الــذُّروة أو مع عدد مرضى كبيــر؛ مما يُحوِّل الثغــرة الســيبرانية المخفيَّة فــي النظام إلى قرار طبــي غير صحيح يُؤثِّر علــى حياة المرضى.

هجمات عبر الموردين

هـي هجمـات سـيبرانية تسـتهدف أنظمـة وشـبكات الموردين (شـركات الأجهـزة الطبيـة/ شـركات الأدويـة/ شـركات التأميـن/ مـزودو السـحابة)، الأساسـيين للوصـول إلـى شـبكة المؤسسـة الطبيـة الرئيسـية.

إستراتيجية الهجوم

يسـتهدف المهاجمون الشـركات الصغيرة المتصلة بالمستشـفى مثل: مُـزوّدي الصيدلـة بدلًا من المستشـفى مباشـرة؛ لأنها أقل حماية وأسـهل اختراقًا، ثم ينتقلون لشـبكة المستشـفى عبر VPN أو اتصال EMR المشـترك.

التأثـير المتتالـي

عندمـا تُصَاب شـركة صيدلـة مركزيـة، تتوقّف إمـدادات الأدوية لـ50 مستشـفى -بحد أدنـى-، متصلة في نفس اللحظـة، ويُطلَب مـن كلّ مستشـفى دَفْع فدية منفصلـة، مما يُحَـوِّل ثغرة واحدة صغيرة إلـى أزمة متعددة المستشـفيات.

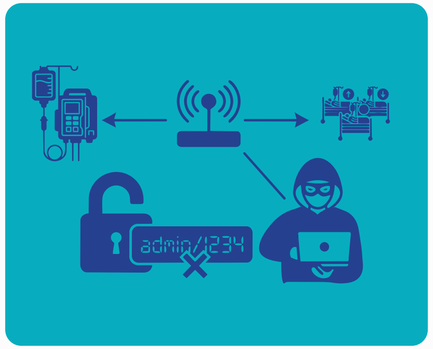
سؤال تفاعلي

لماذا تُعدّ هجمات عبــر الموردين خطيرة على المستشفيات حتى لو كانت أنظمتها محمية؟

اختراق مضخات الأدوية

مضخات الأدوية الوريدية المتصلة تُشكّل خطرًا مميتًا عند اختراقها؛ حيث يستطيع المهاجم تغيير الجرعات عن بُعد؛ مما يُؤدّي للوفاة.

الوصول البسيط للمهاجم



مضخات الأدوية تحتوي كلمات مرور افتراضية "admin/1234" معروفة علنًا، متصلة بنفس شبكة Wi-Fi المستشفى العامة؛ مما يسمح لأيّ شخص داخل المبنى بالوصول لتغيير جرعات عشرات المرضى في وحدة العناية المركزة خلال دقائق.

اختراق كاميرات المراقبة

تَستخدم كاميرات المراقبة في المؤسسات الطبية غالبًا كلمات مرور افتراضية؛ مما يسمح بالتجسُّس على غُرَف المرضى والمناطق المحظور دخولها لغير العاملين.

التجسُّس على الخصوصية الطبية

كاميرات البثّ المباشِر في غُرَف العناية المركزة تَبُثّ مباشرةً على الإنترنت العام من أيّ مكان في العالم، مما يسمح للغرباء بمشاهدة مرضى فاقدي الوعي، عمليات جراحية حساسة، أو أطفال في وحدة العناية المركزة دون علم أحد.

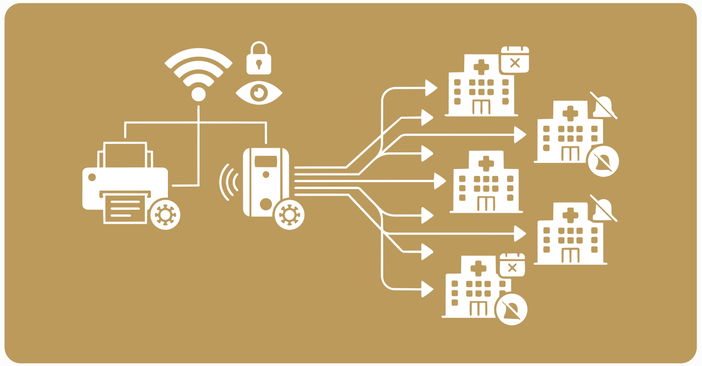
الوصول غير المصرّح به للخرائط

تسجيلات الكاميرات تُظْهِر مخططات داخلية كاملة للمستشفى، مواقع غرف الأدوية، والأبواب الخلفية، وأماكن حراسة الأمن، مما يُعْطِي المهاجمين خارطة طريق للدخول الجسدي أو التخطيط لهجمات مدروسة.

خَرْق الأجهزة الطبية

خَـرْق الأجهـزة الرئيسـية للمؤسسـة الطبيـة (مثـل: الطابعـات أو أجهـزة إنترنـت الأشـياء IoT) قـد يتسـبَّب فـي مهاجمـة مؤسسـات أخـرى ذات صلـة عبـر نَشْـر برمجيـات حَجْـب الخدمـة الموزّعـة، أو برمجيـات أخـرى خبيثـة فـي أجهزتهـا.

الآليـــة



طابعات الأدوية وأجهزة إنترنت الأشـياء الطبية تُصاب ببرمجيات خفية تُهاجم مستشـفيات أخرى بهجمات حجـب الخدمة الموزعة؛ مما يُعطِّـل أنظمة الحجوزات والطوارئ في مؤسسـات طبية أخـرى، بينما تظل الأجهـزة المصابة متصلة بالإنترنت دون كشـف الخطر الحقيقي.

المحور الثالث

أساليب الوقاية والسلامة الرقمية

كلمة المرور

رمز سرّي يُستخدَم للتحقُّق من هوية المستخدِم، وضمان أنّ الوصول إلى الحسابات يتم مِن قِبَل أصحابها فقط.

أهميـــة كلمـــة المـــرور

تمنع الوصول غير المصرّح به إلى الحسابات الرقمية

تحمي البيانات الشخصية والمالية من الاستغلال

تُسهم في الحفاظ على الخصوصية الرقمية للمستخدِم

تَحُدّ من مخاطر انتحال الهوية الإلكترونية

تُعزّز مستوى الأمان العام للخدمات والأنظمة

خصائص كلمة المرور القوية

ألا تَقِلّ عن 8 عناصر تتنوَّع بين الحروف والأرقام والرموز

تحتوي على مزيج من الحروف الكبيرة والصغيرة

غير مرتبطة ببيانات شخصية أو معلومات يمكن توقُّعها

فريدة وغير مستخدَمة في حسابات أخرى

إدارة كلمات المرور

لا تقلّ إدارة كلمات المرور أهميةً عن إنشائها؛ إذ تؤدّي الإدارة غير الصحيحة إلى إضعاف مستوى الحماية.

ممارســات الإدارة الآمِــنة

01 تجنّب كتابة كلمات المرور في أماكن يسهل الوصول إليها

02 عدم حفظ كلمات المرور على الأجهزة دون حماية

03 استخدام وسائل تخزين رقمية مُشفَّرة وآمِنَة

04 الامتناع عن إرسال كلمات المرور عبر وسائل غير آمنة

05 مراجعة كلمات المرور وتحديثها عند الحاجة

أدوات إدارة كلمات المرور

توفر أدوات إدارة كلمات المرور حلولًا عملية لتخزين وإنشاء كلمات مرور قوية بطريقة آمِنَة.

فوائد هذه الأدوات

01 إنشاء كلمات مرور قوية تلقائيًّا

02 تخزين كلمات المرور بشكل مُشفَّر

03 تقليل الاعتماد على التذكُّر اليدوي

04 منع تكرار استخدام كلمات المرور

05 رفع مستوى الأمان العام للحسابات

المصادقة الثنائية البيومترية

تعتمد المصادقة البيومترية على الخصائص الجسدية الفريدة للمُستخدِم كوسيلة تحقُّق إضافية.

مزايا المصادقة البيومترية

01 صعوبة تقليد الخصائص الجسدية للمستخدم

02 سهولة وسرعة في إتمام عملية التحقُّق

03 تقليل الاعتماد على الحفظ والتذكُّر

04 تعزيز الأمان في الأجهزة الذكية

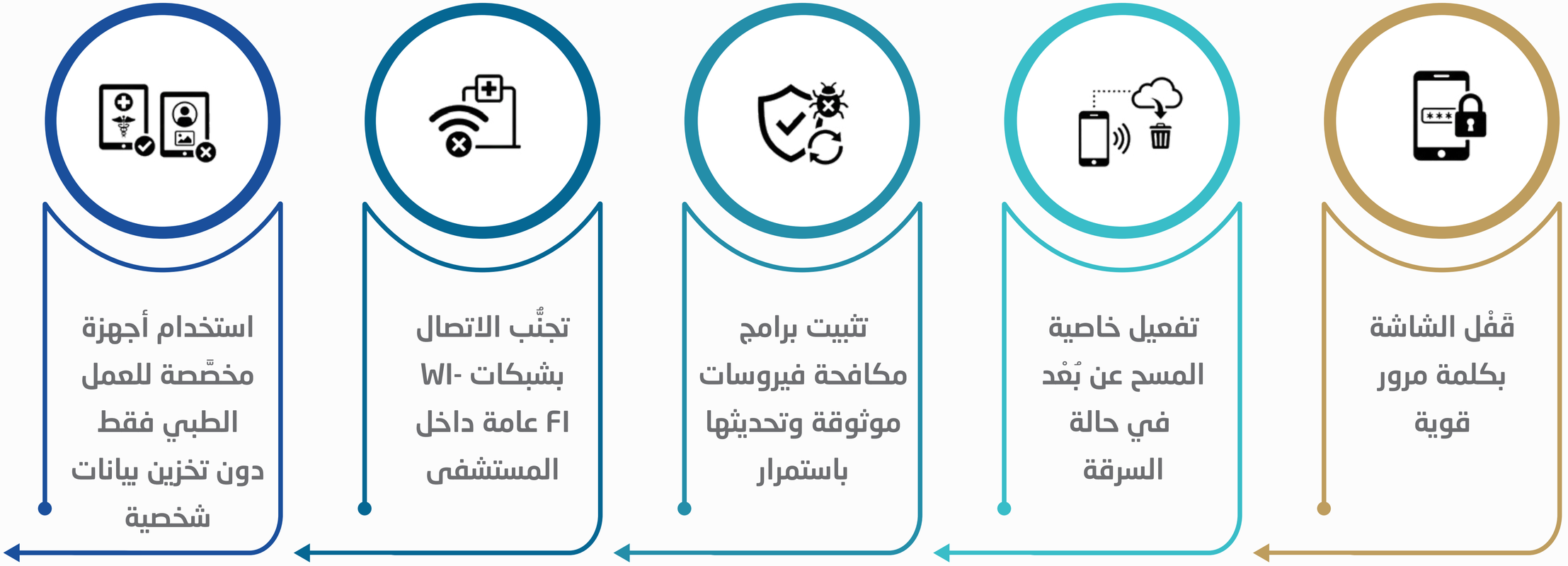
05 رفع مستوى الحماية للحسابات الحساسة

سؤال تفاعلي

ما مزايا المصادقة الثنائية البيومترية مقارنةً بكلمة المرور التقليدية؟

تأمين الأجهزة الشخصية

تأمين الأجهزة الشخصية (مثل: الهواتف والحواسيب) المستخدَمة في المستشفيات يتطلب ممارسات عدة، منها:



التعامل الآمِن مع البريد الإلكتروني

تعزيــز الوعــي الرقمي للأفراد بممارســات التعامل الآمِن مــع مرفقات البريــد الإلكتروني يُقلِّل نســبة نجاح هجمات التصيد بشــكل ملحوظ.

أبرز الممارسات

01
التحقُّق من عنوان المُـرسِل قبل فَتْح المـرفقـــات أو الروابط

02
عـــدم إرســـال معلومات حساسة عبر البريد الإلكتروني

03
الإبلاغ الفوري عن أيّ رسـالة مشبـــوهة

04
استخدام فلاتر البريد الإلكتروني المتقدّمة لكشف التصـــيد

سؤال تفاعلي

ما أفضل الممارسات لتأمين الأجهزة الشخصية

داخل المستشفى؟

تشفير البيانات الطبية

ينبغي تشــفير جميــع البيانات الطبية في أثنــاء التخزين والنقل باســتخدام خوارزميــات قوية مثل AES-256، مع تشــفير الخوادم الرئيســية والأجهزة المحمولــة تلقائيًّا، والتحقُّق الدوري مــن سلامة المفاتيح التشــفيرية مع تخزينها فــي أماكن آمنة.

إدارة الحوادث السيبرانية

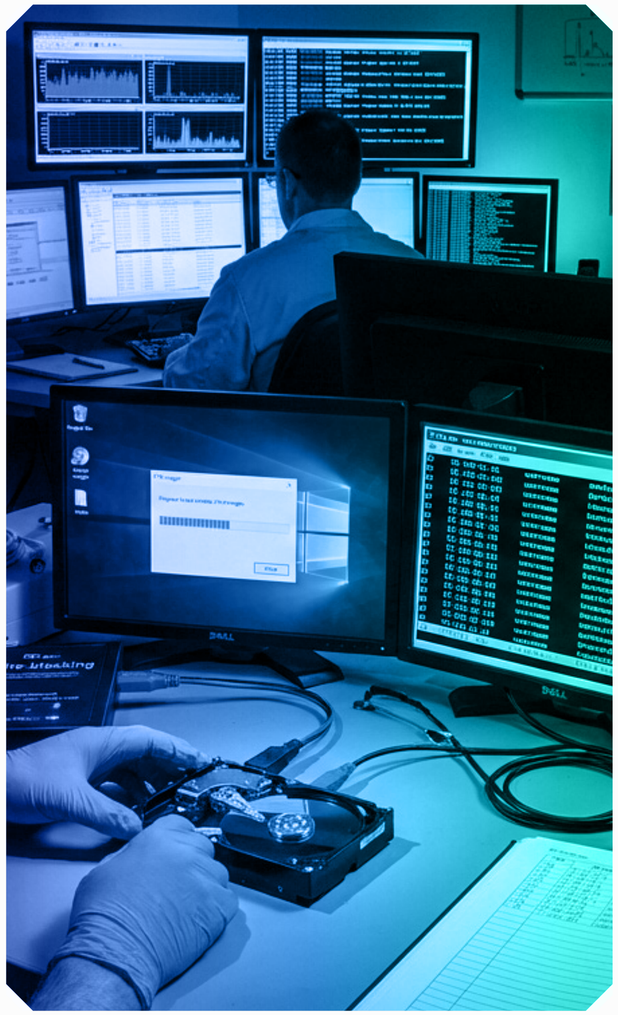
01 تحديد نوع الهجوم فورًا.

02 إيقاف انتشار الهجوم بعَزْل الأجهزة المصابة عن طريق فَصْل الكابلات أو حظر IP.

03 تشكيل فريق استجابة سريع يتكوَّن من خبراء تقنيين وأطباء لتقييم التأثير على الرعاية الطبية

04 توثيق الأدلة الرقمية، وتسجيل لحظة وقوع الحادث (فتح الرسالة، إدخال ذاكرة تخزين).

التحقيق الجنائي وجَمْع الأدلة الرقمية



01

التحقيق الجنائي يبدأ بعَزْل فوري للأجهزة المصابة للحفاظ على سلامة الأدلة، مع إنشاء صورة رقمية كاملة (forensic image) للقرص الصلب باستخدام أدوات مثل FTK Imager

02

يُرَكِّز على استخراج السجلات (logs) من الخوادم وجدران الحماية؛ لتحديد مسار المهاجم وأدواته مثل IP الأصلي، وأسماء المستخدِمين المُستخدَمة

03

جَمْع الأدلة يشمل تحليل الذاكرة العشوائية (RAM) للكشف عن البرمجيات الخبيثة النشطة، مع توثيق كل خطوة في سلسلة الحفظ (chain of custody)

التعافي واستعادة البيانات

01 التعافي يبدأ باختبار النُّسَخ الاحتياطية في بيئة معزولة؛ للتأكد من خلوّها من البرمجيات الخبيثة قبل الاستعادة

02 يُفضَّل استعادة البيانات الحرجة أولًا مثل سجلات العناية المركزة، مع تشغيل الأنظمة على شبكة منفصلة تمامًا

03 الاستعادة التدريجية تتجنَّب إرهاق الخوادم، مع مُراقَبة مستمرة لأيّ نشاط مشبوه في أثناء العملية

04 تُوَثَّق كل خطوة لتقرير الإدارة مع تحديث خطة الطوارئ بناءً على الدروس المستفادة

05 التعاون مع مزوّدي النَّسخ السحابي يُسرِّع الاستعادة إذا كانت البيانات مُشفَّرة ومعزولة بشكل صحيح

النَّسخ الاحتياطي للبيانات

01 النَّسخ الاحتياطي للبيانات يتم عن طريق حِفْظها على أقراص خارجية غير متَّصلة بالشبكة (air-gapped) في وسيط تخزين آمِن

02 يُفْحَص أسبوعيًّا للتأكُّد من سلامته وقابلية البيانات للاستعادة

03 في المستشفيات، يُقْصَر على البيانات الحَرِجَة مثل: سجلات المرضى

04 التخزين السحابي يُشفّر بمفاتيح خاصة، ويُفصَل عن الشبكة الرئيسية

05 الاختبار الشهري يضمن عدم وجود برمجيات خبيثة مختبئة

تقييد الوصول إلى البيانات الطبية

1. مبـدأ تقييـد الوصـول Least Privilege يمنـح الوصـول فقـط للبيانـات الضروريـة للمهمـة.

2. تطبيـق مبـدأ الثقـة الصفريـة Zero Trust يعنـي التحقُّـق مـن الهويـة فـي كل وصـول.

3. مراجعة الوصول كل 6 أشهر مع إلغاء الحسابات القديمة.

سؤال تفاعلي

كيــف يمكــن تقييد الوصــول إلــى البيانات الطبية بطريقــة تضمن الخصوصيــة والأمان؟

المراجع

1. CISA - Cybersecurity & Infrastructure Security Agency Ransomware Guide for Healthcare, on site: https://wwwcisagov/stopransomware/healthcare

2. Cybersecurity Best Practices for Medical Devices, CISA, on site: https://wwwcisagov/topics/cybersecurity-best-practices/medical-devices

3. Cyberattacks on Healthcare, IBM Cost of a Data Breach Report, on site: https://wwwibmcom/reports/data-breach

4. ENISA – European Union Agency for Cybersecurity Cybersecurity for Hospitals and Healthcare, on site: https://wwwenisaeuropaeu/topics/healthcare

5. FBI – Internet Crime Complaint Center Ransomware Targeting Healthcare, on site: https://wwwic3gov/Media/Y2025/PSA250101

6. HHS – Health Sector Cybersecurity Coordination Incident Response Guidelines, on site: https://wwwhhsgov/sites/default/files/health-sector-cybersecurity-coordinationpdf

7. HIPAA Journal Healthcare Data Breaches and Fines, on site: https://wwwhipaajournalcom/healthcare-data-breach-statistics/

8. INTERPOL Cybercrime Against Healthcare Targets, on site: https://wwwinterpolint/Crimes/Cybercrime/Cyber-threats

9. Microsoft Security Blog RansomHub Ransomware Analysis, on site: https://wwwmicrosoftcom/security/blog/ransomhub

10. NCSC – UK National Cyber Security Centre Healthcare Cyber Security Guidelines, on site: https://wwwncscgovuk/guidance/healthcare-sector

11. NIST – National Institute of Standards and Technology Cybersecurity Framework for Healthcare, on site: https://wwwnistgov/cyberframework/healthcare
12. Sophos State of Ransomware in Healthcare, on site: https://wwwsophoscom/en-us/content/state-of-ransomware-healthcare
13. Splunk SIEM for Healthcare Security, on site: https://wwwsplunkcom/en_us/solutions/healthcare/siemhtml
14. Trend Micro Qilin Ransomware Threat Report, on site: https://wwwtrendmicrocom/vinfo/us/security/news/ransomware-spotlight/qilin
15. US-CERT RDP Vulnerabilities and Mitigation, on site: https://wwwus-certgov/ncas/alerts/TA17-075A
16. WHO – World Health Organization Cybersecurity in Health, on site: https://wwwwhoint/health-topics/cybersecurity
17. CISA Endpoint Detection and Response (EDR) Guidance, on site: https://wwwcisagov/topics/cybersecurity-best-practices/edr
18. Health-ISAC Coordinated Healthcare Incident Response, on site: https://health-isacorg/chirp
19. Fortinet Network Segmentation Best Practices, on site: https://wwwfortinetcom/resources/cyberglossary/network-segmentation
20. CrowdStrike Double Extortion Ransomware Tactics, on site: https://wwwcrowdstrikecom/cybersecurity-101/ransomware/double-extortion/
21. Checkpoint Research RansomHub Technical Analysis, on site: https://researchcheckpointcom/2024/ransomhub/
    1. https://healthsectorcouncilorg/wp-content/uploads/2023/07/HIC-CHIRP-FINAL_1pdf
    2. https://filesasprtraciehhsgov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-responsepdf
    3. https://wwwahaorg/system/files/media/file/2023/05/health-industry-cybersecurity-tactical-crisis-response-hic-tcr-may-2020pdf
    4. https://oehicoloradogov/health-information-cybersecurity

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 40466379 - 51045944

www.ncsa.gov.qa academy@ncsa.gov.qa