

دراسات نقدية ١

الباحث/عبدالسلام العتيبي

الأسبوع السابع



دراسات نقدية ١

Mitigating Cybersecurity Risks in the U.S. Healthcare Sector

إعداد
الباحث/عبدالسلام العتيبي

في عصر التكنولوجيا الرقمية المتقدمة، أصبح القطاع الصحي في الولايات المتحدة يعتمد بشكل متزايد على الأنظمة الإلكترونية لإدارة السجلات الصحية، ومراقبة المرضى، وتسهيل الوصول إلى المعلومات الطبية. ولكن مع هذا التوسع الكبير في استخدام التكنولوجيا، ظهرت تحديات كبيرة تتعلق بالأمن السيبراني. تعرضت العديد من المؤسسات الصحية في الآونة الأخيرة لتهديدات سيبرانية متنوعة، مثل هجمات الفدية (Ransomware)، وتسريب البيانات، واختراق الأنظمة الحساسة، مما يهدد أمن بيانات المرضى وسرية المعلومات الصحية. هذه الهجمات لا تؤثر فقط على خصوصية الأفراد، بل تهدد أيضًا سلامة النظام الصحي بشكل عام، بما في ذلك توقف الخدمات الطبية وتدمير الثقة العامة في المؤسسات الصحية وتعد حماية المعلومات الصحية الشخصية أمرًا بالغ الأهمية في ظل القوانين واللوائح الصارمة مثل قانون **HIPAA** (قانون التأمين الصحي القابل للنقل والمساءلة) في الولايات المتحدة، الذي يفرض تدابير أمنية لحماية البيانات الصحية الإلكترونية. على الرغم من الجهود المبذولة، فإن القطاع الصحي ما زال يواجه تحديات مستمرة في تطوير استراتيجيات فعالة للتصدي للمخاطر السيبرانية المتزايدة ويهدف هذا البحث إلى دراسة المخاطر السيبرانية التي تهدد القطاع الصحي الأمريكي، وتقديم حلول عملية للحد منها. من خلال تحليل التهديدات الحالية، تقييم السياسات الأمنية المتبعة، ومقارنة استراتيجيات الأمان بين المؤسسات الصحية المختلفة، يسعى البحث إلى تقديم رؤى عملية لتحسين مستويات الأمان السيبراني في القطاع الصحي. كما يتناول البحث أهمية تعزيز الوعي الأمني بين الموظفين، وتطوير تقنيات جديدة مثل الذكاء الاصطناعي في الكشف عن الهجمات السيبرانية، لضمان حماية البيانات الصحية وسلامة النظام الصحي وتتضمن الدراسة تحليل البيانات من تقارير الحوادث الأمنية، مقابلات مع خبراء في مجال الأمان السيبراني، ودراسات حالة لمؤسسات صحية تعرضت لتهديدات سيبرانية. من خلال هذه الدراسة، سيتم تحديد الفجوات الأمنية التي تواجه المؤسسات الصحية واقتراح استراتيجيات للتحسين، بما في ذلك تعزيز الإجراءات الوقائية، تدريب الموظفين، واستخدام التكنولوجيا المتطورة في مواجهة المخاطر السيبرانية.

يتبنى الباحث في هذا البحث منهجاً مختلطاً يجمع بين **المنهج الوصفي التحليلي** و **المنهج التقييمي** لتقديم تحليل شامل لمخاطر الأمن السيبراني في القطاع الصحي الأمريكي، ووضع حلول عملية للحد منها. يتضمن النموذج التالي عدة جوانب:

١. **المنهج التحليلي:** تحليل التهديدات السيبرانية التي تواجه المؤسسات الصحية، مثل الهجمات الإلكترونية، الفيروسات، والبرمجيات الخبيثة ودراسة البيانات المتعلقة بحوادث الاختراق السابقة في المؤسسات الصحية الأمريكية وتحديد الأنماط المتكررة للهجمات السيبرانية، وبيان التأثير الذي تخلفه على النظام الصحي.
٢. **المنهج الوصفي:** وصف الوضع الراهن للأمن السيبراني في القطاع الصحي، بما في ذلك الإجراءات والتقنيات المتبعة من قبل المؤسسات الصحية لمواجهة التهديدات وتقييم مدى تأثير هذه الإجراءات على حماية البيانات الصحية.
٣. **المنهج التقييمي:** تقييم فعالية السياسات الأمنية الحالية، مثل استخدام أنظمة الكشف عن التسلل، التشفير، والتوثيق متعدد العوامل.
٤. **المنهج التوجيهي:** تقديم توصيات وحلول عملية للمؤسسات الصحية لتعزيز الأمان السيبراني واقتراح استراتيجيات للمؤسسات الصحية الصغيرة التي تفتقر إلى الموارد الكافية لتبني الحلول المتقدمة وتقديم حلول مبتكرة مثل استخدام تقنيات الذكاء الاصطناعي لتحسين الكشف المبكر عن الهجمات.
٥. **المنهج الوقائي:** تسليط الضوء على أهمية الوقاية ومنع الهجمات بدلاً من الاكتفاء بالاستجابة بعد وقوع الهجوم ودراسة كيفية تنفيذ استراتيجيات الأمان الوقائي مثل التشفير على جميع مستويات الأنظمة الصحية.

تتيح الدراسات الميدانية للباحث جمع بيانات واقعية وعملية تساعد في فهم التحديات الفعلية التي تواجه المؤسسات الصحية في الولايات المتحدة في مجال الأمن السيبراني. كما أنها تساهم في تقييم استراتيجيات الأمان المستخدمة، وتزود الباحث بتوصيات قابلة للتطبيق لتحسين السياسات والإجراءات الأمنية باستخدام الدراسات الميدانية، يمكن للباحث تقديم توصيات مستندة إلى بيانات حقيقية ومقارنة بين المؤسسات الصحية المختلفة، مما يزيد من قوة وواقعية النتائج المستخلصة من البحث الدراسات الميدانية التي قد يعتمد عليها الباحث في هذا النوع من البحث:

دراسات حالة للمؤسسات الصحية: تحليل حالات حقيقية لمؤسسات صحية أمريكية تعرضت لتهديدات سيبرانية مثل الهجمات بالفيروسات أو الفدية (Ransomware) أو تسريبات البيانات.

استطلاعات رأي المؤسسات الصحية: جمع بيانات عن كيفية تصدي المؤسسات الصحية الأمريكية لمخاطر الأمن السيبراني، والتعرف على مدى وعيها بالأخطار وأدوات الأمان المتاحة.

تحليل البيانات الأمنية من تقارير الحوادث: (Incident Reports) تحليل البيانات المجمعة من تقارير الحوادث الأمنية التي سجلت في المؤسسات الصحية.

مقابلات مع خبراء في الأمان السيبراني: الحصول على رؤى معمقة من الخبراء في الأمان السيبراني الذين يعملون في القطاع الصحي.

تحليل السياسات الأمنية في المؤسسات الصحية: فحص مدى تطبيق السياسات والإجراءات الأمنية في المؤسسات الصحية.

دراسة مقارنة بين المؤسسات الصحية الكبرى والصغرى: مقارنة طرق حماية الأمن السيبراني بين المستشفيات الكبرى والصغيرة.



Thank You