|  |
| --- |
| **الجمهورية اللبنانية** |
| **وزارة الأشغال العامة والنقل** |
| **مصلحة إستثمار مرفأ طرابلس** |

**دفتر الشروط الفني لأعمال " حماية الأمن السبراني في مرفأ طرابلس "**

**مقدمة**

الأمن السبراني هو مجموعة من الإجراءات والسياسات والتقنيات والممارسات التي تهدف وتُصمم لحماية الأنظمة المعلوماتية والشبكات السلكية واللاسلكية والفايبر أوبتيك والبيانات من التهديدات السبرانية والهجمات والإختراقات الإلكترونية. يهدف الأمن السبراني إلى توفير سرية، سلامة البيانات والمعلومات الرقمية للمؤسسات والأفراد.

نذكر على سبيل المثال لا الحصر بعض التفاصيل عن مكونات وأهداف الأمن السبراني:

1. السرية (Confidentiality) : تتعلق بالحفاظ على سرية البيانات والمعلومات لضمان عدم الوصول إليها أو التلاعب بها من قبل أطراف غير مخولة.
2. السلامة (Integrity) : تتعلق بالحفاظ على سلامة البيانات والمعلومات من التلاعب أو التغيير غير المصرح به، سواء بشكل عفوي أو متعمد.
3. التوافر (Availability) : يهدف إلى ضمان توفر الخدمات والبيانات للمستخدمين المصرح لهم في الوقت المناسب دون تعطل أو انقطاع غير مخطط له.
4. المصداقية (Authenticity) : يتعلق بالتأكد من هوية الأشخاص والأنظمة والبيانات للتحقق من صحة المعلومات ومصداقيتها.
5. غير الرفض (Non-Repudiation): يتعلق بتوفير دليل قانوني على العمليات والتحولات التي تمت داخل النظام لتمكين التحقق من الأنشطة ومنع الإنكار.
6. المتانة (Resilience) : يهدف إلى تعزيز قدرة النظام على المقاومة والتعافي من الهجمات والأحداث السلبية.

تتضمن إستراتيجيات الأمن السبراني مجموعة متنوعة من التقنيات والسياسات والتدابير الوقائية والإستجابية لمواجهة التهديدات السبرانية. تشمل هذه التقنيات والتدابير الحماية النشطة مثل جدران الحماية وأنظمة الكشف عن الاختراق، وكذلك السياسات والتدابير الوقائية مثل التدريب على الوعي الأمني وإدارة الهويات والوصول.

2

بإختصار، يمثل الأمن السبراني جزءاً حيوياً من عالم التكنولوجيا الحديثة، حيث يساعد في حماية الأنظمة والبيانات الرقمية من التهديدات المتزايدة والمتطورة في العصر الرقمي. تهدف جميع هذه الجوانب إلى توفير بيئة آمنة للمعلومات والبيانات والتأكد من سلامتها وسرية وسلامة البيانات الحساسة والمعلومات الحيوية للمؤسسات والأفراد.

يشمل مجال الأمن السبراني العديد من الجوانب والتحديات التي يجب مواجهتها وحماية الأصول الرقمية منها. نذكر

منها:

أ- حماية الأنظمة والشبكات السلكية واللاسلكية والفايبر أوبتيك: يتضمن الأمن السبراني تنفيذ تدابير وسياسات لحماية

أنظمة المعلومات والشبكات السلكية واللاسلكية والفايبر أوبتيك من الاختراقات والتهديدات الخارجية والداخلية.

ب- الكشف عن التهديدات: يشمل البحث والكشف عن الأنشطة غير المشروعة والتهديدات السبرانية المحتملة داخل

البنية التحتية للمؤسسة.

ج- الوقاية من الهجمات: يتعلق هذا باتخاذ التدابير الوقائية لتقليل مخاطر الهجمات السبرانية مثل تحديث البرمجيات

بانتظام وتطبيق تقنيات الحماية النشطة.

د- الاستجابة للحوادث: يتضمن إستجابة فعالة وسريعة للحوادث الأمنية مثل الإختراقات وإنتهاكات البيانات، بما في

ذلك التحقيق وإدارة الأزمات وإستعادة البيانات.

ه- التوعية والتدريب: يتضمن التركيز على توعية المستخدمين بأمان المعلومات وتوفير التدريب المناسب لهم للحد

من المخاطر الأمنية.

ح- الإمتثال والتشريعات: يتعلق بالإلتزام بالتشريعات والمعايير الأمنية المحلية والدولية، وضمان مطابقة المؤسسة

لهذه المتطلبات.

ط- التقييم والتحسين المستمر: يشمل التقييم المنتظم لسياسات الأمان والتقنيات والإجراءات، مع التركيز على تحسينها

باستمرار لمواجهة التهديدات المتغيرة.

نسرد بعض المتطلبات والمهارات العامة للعاملين ضمن مجال الأمن السبراني:

- خبرة في مجال الأمن السبراني سواء من خلال العمل العملي أو المشاركة في مشاريع أمنية، مع درجة في مجال

تكنولوجيا المعلومات أو أمن المعلومات.

- مهارات إتصال ممتازة للتفاعل مع فرق العمل وشرح التحديات الأمنية والحلول المقترحة كما يجب أن يكون لديه

القدرة على كتابة تقارير فنية ووثائق توثيقية.

- القدرة على تحليل سجلات النشاط الشبكي وتحديد الهجمات والتهديدات المحتملة كما يجب أن يكون لديه القدرة على

الإستجابة الفورية للحالات الطارئة وإدارة الأزمات الأمنية.

3

- القدرة على التعلم المستمر ومتابعة التطورات في مجال الأمن السبراني، والقدرة على توجيه وتدريب فرق العمل

الأخرى بشأن ممارسات أمن المعلومات والإستجابة لحوادث الأمن مع القدرة على التعامل مع التهديدات المتقدمة

والهجمات المتطورة والهجمات الهجينة.

- خبرة في إدارة أمن المعلومات والشبكات السلكية واللاسلكية والفايبر أوبتيك وإعداد سياسات الأمن وتقييم المخاطر

وإدارة الهويات والوصول وفي تنفيذ وإدارة حلول التحقق من الهوية وإدارة الوصول.

- معرفة بتقنيات إختبار الإختراق لتقييم نقاط الضعف في الأنظمة والشبكات السلكية واللاسلكية والفايبر أوبتيك

والتطبيقات، معرفة بتقنيات إكتشاف الإختراق وإستجابة الطوارئ السبرانية مع خبرة في إستخدام أدوات الإختراق

الأخلاقية لإختبار أمان النظام.

- معرفة بأمن تطبيقات الويب والهجمات الشائعة وبالتهديدات الأمنية المتعلقة بالبيئات السحابية وبالتقنيات الناشئة في

مجال الأمن وتقنيات التحليل الضخم والذكاء الاصطناعي (AI) وتطبيقاتها في مجال الأمن السبراني.

- معرفة عميقة بأساسيات أمن المعلومات وتقنيات التشفير، مع فهم واسع للثغرات الأمنية والهجمات السبرانية

المحتملة، ومعرفة بالتشريعات واللوائح الخاصة بأمن المعلومات والخصوصية، والإلتزام بالمعايير الأمنية المعترف

بها عالميًا.

- قدرة على تصميم وتنفيذ استراتيجيات أمان فعالة للشبكات والأنظمة، مع قدرة على تطوير وتنفيذ سياسات

وإجراءات الأمن وتدريب الموظفين عليها.

- مهارات تحليلية قوية لرصد واكتشاف الأنشطة الغير مشروعة على الشبك مع مهارات تقنية ومعرفة عميقة بأنظمة

التشغيل المختلفة بالإضافة إلى فهم لغات البرمجة مع فهم جيد للشبكات السلكية واللاسلكية والفايبر أوبتيك

وبروتوكولاتها.

**المواصفات الفنية المطلوبة لفريق الإشراف:**

1. مهندس أمن سيبراني:

* Strong understanding of network security principles, protocols, and technologies.
* Proficiency in penetration testing, vulnerability assessment, and security auditing.
* Expertise in configuring and managing firewalls, intrusion detection/prevention systems (IDS/IPS), and security information and event management (SIEM) systems.
* Knowledge of encryption techniques and cryptographic protocols.
* Familiarity with various operating systems (Windows, Linux, Unix) and their security mechanisms.
* Experience with security assessment tools such as Metasploit, Nessus, Nmap, and Wireshark.
* Understanding of secure coding practices and web application security.
* Ability to conduct security incident response and forensic analysis.
* Knowledge of regulatory compliance requirements (e.g., GDPR, HIPAA, PCI DSS).
* Strong communication and interpersonal skills to effectively interact with clients and stakeholders.
* Additionally, certifications like Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), or GIAC Security Expert (GSE) may be beneficial.
* أن يكون حائزاً على شهادة الهندسة في الحاسوب أو المعلوماتية أو الأمن السبراني أو ما يعادلها.
* أن يكون مسجل في نقابة المهندسين منذ اكثر من عشر سنوات .
* أن يكون لديه خبرة في الأعمال الإستشارية المتعلقة في نظم الأمن السبراني لمدة لا تقل عن 5 سنوات.

1. مهندس الشبكات السلكية واللاسلكية والفايبر أوبتيك:

* Expertise in network design, implementation, and troubleshooting across various technologies such as: Routing and switching protocols (e.g., OSPF, BGP, VLANs).
* Network security principles and technologies (e.g., firewalls, VPNs, intrusion detection/prevention).
* Wireless networking standards and protocols (e.g., 802.11ac, WPA2, WPA3).
* Network monitoring and management tools (e.g., SNMP, NetFlow, Wireshark).
* Cloud networking concepts and technologies (e.g., SD-WAN, VPCs, Azure Virtual Network).
* Network virtualization technologies (e.g., VMware NSX, Hyper-V Network Virtualization).
* Software-defined networking (SDN) principles and implementations.
* IPv4 and IPv6 addressing and subnetting.
* Network hardware from various vendors (e.g., Cisco, Juniper, Arista).
* VoIP and unified communications protocols (e.g., SIP, RTP, H.323).
* Additionally, strong communication skills, problem-solving abilities, and the capability to understand and address clients' specific networking needs are essential for a successful consultant engineer in networking.
* أن يكون حائزاً على شهادة الهندسة في الحاسوب أو المعلوماتية أو الشبكات (الشبكات السلكية واللاسلكية والفايبر أوبتيك) أو ما يعادلها.
* أن يكون مسجل في نقابة المهندسين منذ اكثر من عشر سنوات .
* أن يكون لديه خبرة لا تقل عن 5 سنوات في الأعمال الإستشارية المتعلقة بالشبكات.

1. فني معلوماتية وشبكات سلكية ولاسلكية وفايبر أوبتيك :

* Networking: Proficiency in networking concepts such as TCP/IP, routing, switching, VLANs, VPNs, firewalls, DNS, DHCP, etc.
* Operating Systems: Understanding of various operating systems like Windows, Linux, and Unix, including their security features and configurations.
* Cybersecurity: Knowledge of cybersecurity principles, including threat detection, prevention, and mitigation techniques. Familiarity with common security tools like IDS/IPS, SIEM, antivirus, and penetration testing tools.
* Encryption and Cryptography: Understanding of encryption algorithms, cryptographic protocols, and their applications in securing data and communications.
* Risk Assessment and Management: Ability to assess security risks, develop risk management strategies, and implement appropriate controls to mitigate risks.
* Compliance and Regulations: Awareness of relevant laws, regulations, and industry standards (e.g., GDPR, HIPAA, PCI DSS) related to cybersecurity and data protection.
* Incident Response: Knowledge of incident response procedures, including incident detection, analysis, containment, eradication, and recovery.
* Ethical Hacking: Familiarity with ethical hacking techniques and tools to identify vulnerabilities and assess the security posture of systems and networks.
* Cloud Computing Security: Understanding of cloud computing concepts and security considerations in cloud environments, including IAM (Identity and Access Management), data encryption, and secure configurations.
* Monitoring and Auditing: Experience with security monitoring tools and techniques for detecting and responding to security incidents. Ability to conduct security audits and assessments to ensure compliance with security policies and standards.
* Effective communication, problem-solving abilities, and a proactive approach to learning and staying updated with the latest cybersecurity trends and threats are also essential for a consultant technician in cybersecurity and networking.
* Providing technical support to employees, handling error, detects and repairs it.
* Save data and backed up regularly
* Coordinating with programming companies and preparing the necessary resources for the programs.
* Adopting policies and procedures that enable every employee to access the computer system and information in accordance with security standards.
* أن يكون حائزاً على شهادة بكالوريوس حاسوب أو شبكات (شبكات سلكية ولاسلكية وفايبر أوبتيك) أو ما يعادلها.
* أن يكون لديه خبرة في نظم الحماية السبرانية والشبكات (شبكات سلكية ولاسلكية وفايبر أوبتيك) لا تقل

عن 5 سنوات.