الجمع بين
صمام البيانات وجدران
حماية الشبكة

لتحسين
أمن البيانات

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

www.aecl.com

technology developed with
أرامكو السعودية
saudi aramco

المحتويات

ملخص
تنفيذي

تستثمر الشركات والهيئات الحكومية والقطاعات الرئيسية الأخرى بقوة في البنية التحتية للأمن السيبراني حيث من المتوقع أن تصل الخسائر السيبرانية إلى 6 تريليون دولار سنويا بحلول عام 2021. [1] وقد أدت الثورة الرقمية المستمرة إلى زيادة استخدام الخدمات السحابية وأمن الخدمات السحابية والهواتف الذكية وإنترنت الأشياء. [2] وأدى ذلك إلى ظهور عدد كبير من تهديدات الأمن السيبراني المعقدة التي لم تكن موجودة قبل بضعة عقود. وفي الآونة الأخيرة، شهد الشرق الأوسط زيادة في الهجمات الإلكترونية ونشاط القرصنة، بسبب زيادة اعتماد الحلول الرقمية والذكية عبر البنوك والمؤسسات المالية والبنى التحتية الحيوية الأخرى. [3]

وكجزء من رؤية 2030، تعمل المملكة العربية السعودية بشكل دؤوب من أجل إنجاز مختلف مبادرات التوطين والرقمنة. وقد أعطت المملكة الأولوية لمبادراتها في مجال الأمن السيبراني لتطوير شبكة حماية فيما يتعلق بأنظمة التحكم والبنية التحتية الرقمية والأجهزة الذكية والعمليات الأخرى ذات المهام الحيوية. [4]

يعتبر الوضع الحالي للأمن السيبراني أكثر أهمية من أي وقت مضى حيث أصبحت الهجمات الإلكترونية أكثر عدوانية وقوة. وأدى زيادة استخدام أجهزة إنترنت الأشياء أيضا إلى توسيع مساحة الهجوم. لذلك فمن المهم بالنسبة للقطاعات الرائدة والصناعات الحيوية أن تتبنى التقنيات السيبرانية التي قد توفر حماية مضمونة ضد الهجمات والاختراقات والجرائم. وقد طورت شركة الإلكترونيات المتقدمة، من خلال تخصصها الأساسي في مجال الأمن السيبراني، تقنية صمام البيانات المحلي لحماية البيانات ونقل المعلومات بسرعة. وتم تحسين صمام البيانات المقدم من شركة الإلكترونيات المتقدمة لحماية البنية التحتية الحيوية في المملكة والمناظر الصناعية المتنوعة والتقنيات الرقمية المتنامية.

من الجدير بالذكر أن جدران الحماية ظلت مكونًا مهمًا لأمن البيانات. ومع ذلك، يجب تصحيح جدران الحماية وتحديثها بشكل منتظم للتخلص من احتمال الخطأ والتثبيت الخاطئ. ويتم تعديل صمام البيانات المقدم من شركة الإلكترونيات المتقدمة للعمل جنبًا إلى جنب مع جدران الحماية من خلال التغلب على المشكلات الأساسية في جدران الحماية. ويستخدم صمام البيانات للفصل الفعلي بين المضيف والوجهة لمنع البرامج الضارة الخارجية من دخول الشبكة. إلى جانب ذلك، تم تحسين التقنية بغرض نقل البيانات أحادية الاتجاه لتسهيل التدفق الآمن للبيانات من الشبكات الآمنة إلى الشبكات غير الآمنة والعكس. [5] وبتزايد عدد الشبكات المعرضة لنقاط الضعف كل يوم، يوفر صمام البيانات إضافة قيمة محتملة إلى مجموعة أدوات الأمن السيبراني الحالية. [5]

تدفق المعلومات
في العالم الرقمي

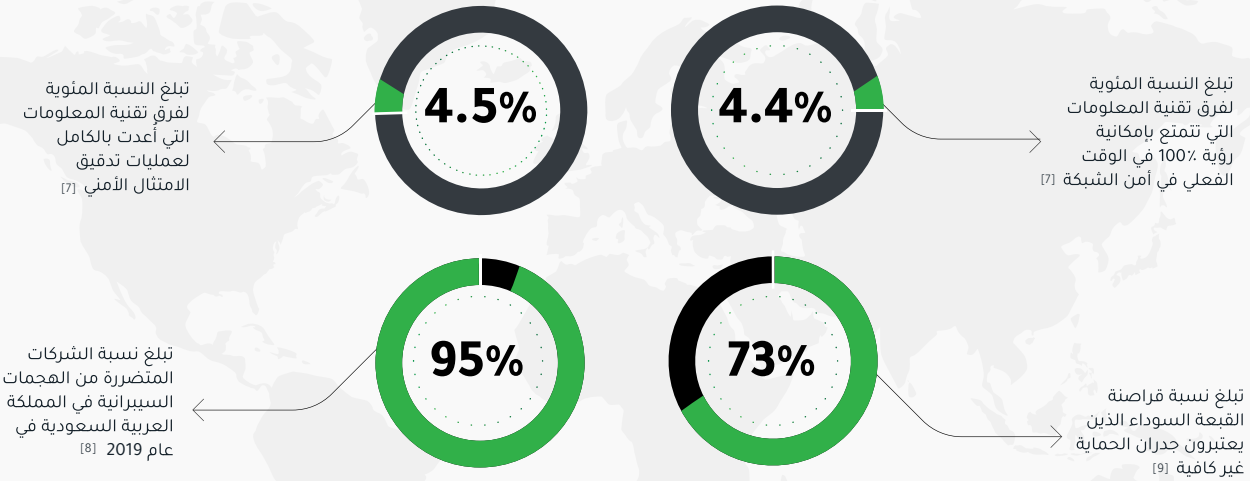
أدى التحول الرقمي إلى زيادة إنترنت الأشياء الصناعي وتدفق المعلومات عبر شبكات الأعمال. [5] وتتضمن هذه الشبكات شبكات التحكم في العمليات وشبكات المؤسسات التي تراقب أنظمة التحكم الصناعية بشكل جماعي .

يؤدي استخدام بروتوكولات الاتصال القياسية عبر الشبكات عالية القيمة إلى تعريض مكونات البنية التحتية الحيوية للهجمات السيبرانية. [6] وتخزن هذه الشبكات البيانات المهمة التي يجب حمايتها من الوصول غير المصرح به، مع ضمان تمكين تدفقات البيانات المناسبة للمستخدمين المصرح لهم من تلقي هذه البيانات. [6]

يمكن لعدد من موجهات الهجوم مثل مرفقات البريد الإلكتروني والبرامج الضارة والفيروسات وصفحات الويب والرسائل الفورية والهندسة الاجتماعية والوصول عن بُعد الدخول إلى الشبكة لتعطيل العمليات أو سرقة البيانات أو بدء الاستخدام غير القانوني. ومن ثم، فمن الضروري أن تحافظ الشركات والمؤسسات على سلامة الشبكات عالية القيمة وسريتها وسلامتها. [5]

تستدعي حماية الشبكات الأمنية مرور البيانات عبر جدران حماية الشبكة. [3] ومع ذلك، فقد أثارت نقاط الضعف في جدران الحماية مخاوف تتعلق بأمان الشبكة. وفي هذا السيناريو، يمكن دمج صمام البيانات مع أمان جدار الحماية لضمان الحماية المثلى ضد الهجمات الخارجية وخروقات البيانات .

حالة البيانات وأمن الشبكات عبر المؤسسات



تشير الأرقام المذكورة أعلاه إلى الحاجة إلى تقنيات أكثر قوة وأمانًا لحماية شبكات البيانات. ويمكن للشركات أن تكمل أمان جدار الحماية الخاص بها من خلال صمام بيانات مرن وذكي يمكنه زيادة رؤية الشبكة وأمانها .

الدمج

بين جدران الحماية وصمام البيانات للحصول على

أمان بيانات بلا عيوب

تجمع جدران حماية الشبكة بين مجموعات القواعد المعقدة لتصفية المعلومات الواردة وتقييد التهديدات المحتملة. [10] ومع ذلك، على الرغم من الفعالية المثبتة لجدران حماية الشبكة في العديد من المجالات إلا أن آلية الاتصال ثنائية الاتجاه الخاصة بها تعرض شبكات الأمان للعديد من ناقلات التهديد .

لمعالجة المشكلات المذكورة أعلاه، تجمع الشركات أوجه التآزر بين جدران الحماية وصمامات البيانات أحادية الاتجاه التي تعزل الشبكة تمامًا عن التهديدات الخارجية والبرامج الضارة والاختراقات .

صمام البيانات - الارتقاء بمستوى أمان البيانات

يمكن إدارة نقاط الضعف في جدران حماية الشبكة بشكل فعال من خلال استخدام صمام البيانات القائم على الأجهزة التي تكمل السابق .

جدار الحماية

قد تسمح التثبيتات الخاطئة لجدار الحماية لبرامج التجسس والبرامج الضارة بتجاوز جدران الحماية واختراق الشبكة .

يمكن توجيه حركة المرور عبر جدار الحماية إلى أجهزة كمبيوتر أخرى ضمن شبكة موثوقة. [11]

تحتوي جدران الحماية على مجموعة قواعد برمجيات معقدة يمكن تنفيذها ويمكن أن تؤخر مدة انتظار الشبكة. [10]

تتطلب جدران الحماية تصحيحًا واعيًا ومراقبة مستمرة وتقييمًا لقاعدة الضبط للحفاظ على الأمان. [13]

تكلفة التشغيل طويلة الأجل للمحافظة على قواعد جدار الحماية والبرامج الدائمة وتدقيقها بمرور الوقت مرتفعة. [10]

يمكن الوصول إليها بسهولة من جانب القراصنة لتطوير ثغرات أمنية. [14]

صمام البيانات

يعالج صمام البيانات الخلل عن طريق ضمان الفصل الفعلي للمضيف والوجهة وحظر البرامج الضارة. ولم يتم الإبلاغ عن أي حالات حدث فيها تجاوز صمام البيانات أو استغلاله لتمكين الإرسال ثنائي الاتجاه. [10]

إن المرور عبر قنوات الألياف البصرية بروتوكول خاص غير قابل للتوجيه ولا يمكنه تنفيذ حزمة بروتوكول التحكم بالنقل/بروتوكول الإنترنت. [10]

يسمح صمام البيانات بتدفق البيانات في الوقت الفعلي دون تأخر في زمن الاستجابة. [12]

ويعمل صمام البيانات دون مجموعة قواعد برمجيات للإعداد والضبط ويصعب تنفيذها بشكل خاطئ ونادرًا ما تتطلب تغييرات ويسهل مراجعتها نسبيًا. [10]

ويمكن للشركات تثبيت عدد أقل من جدران الحماية والاستثمار في تقنية صمام البيانات بغرض تحسين الالتزام الأمني .

ويصعب على القراصنة السيطرة على صمام بيانات من الدرجة الصناعية مما يزيد من صعوبة تطوير ثغرات أمنية. [10]

إضافة مستوى جديد

من الحماية نتيجة التثبيت الخاطئ لجدران الحماية

على الرغم من التعقيدات الواضحة في جدران الحماية، تثق المؤسسات حول العالم في الوضع الأمني للتقنيات التي تستند إلى برمجيات. ومن خلال الامتثال والمراقبة والإعداد المناسبين، يمكن أن تثبت جدران الحماية بالفعل أنها تقنية قوية لحماية البيانات. ومع ذلك فإن الإعدادات الخاطئة لجدار الحماية أمر شائع في العديد من شبكات الأعمال المهمة.

ستقع 99٪ من اختراقات جدار الحماية بسبب أخطاء في إعدادات جدار الحماية حتى عام 2023. [7]

تمتلك 3 فقط من أصل 10 شركات رؤية أكثر من 80٪ في شبكات جدار الحماية الخاصة بها. [7]

تستخدم 30٪ من الشركات أكثر من 100 جدار حماية. [7]

تستخدم 78٪ من الشركات أكثر من 3 موردين لتنفيذ جدران الحماية. [7]

أدت زيادة عدد جدران الحماية المستخدمة عبر الشبكات التنظيمية، إلى جانب كونها عرضة للتثبيت الخاطئ، إلى تقليل الرؤية في حماية الشبكات. وفي هذا السيناريو، ظهر استخدام صمام البيانات للحماية المضمونة ضد خروقات البيانات كأسلوب أمني إلى جانب جدران الحماية .

وفيما يلي أبرز التحديات التي واجهة المؤسسات في إدارة جدران الحماية :

يتفق العديد من الخبراء الأمنيين مع فكرة استخدام جدران الحماية بالاشتراك مع صمام البيانات من أجل ضمان الأمن الأمثل للبيانات. وعلى سبيل التقييم، لم يتم الإبلاغ عن أي حالات وقع فيها تجاوز صمام البيانات أو استغلاله لتمكين الإرسال ثنائي الاتجاه. [15]

الانتقال من
الفجوات الهوائية إلى جدران الحماية وصمام البيانات

تتغير ناقلات الهجوم في الفضاء السيبراني باستمرار مما يمنح القراصنة صلاحية أكبر في التحكم في الشبكات الأمنية واختراقها. ويتعين على شبكات الأعمال تخطيط رحلة الأمن السيبراني وتحقيق التوازن الكافي في .استخدام الفجوات الهوائية وجدران الحماية وصمام البيانات .

تبادل المعلومات التقليدي للكتل الأمنية الخاصة بالفجوات الهوائية

تمثل الفجوات الأمنية حواجز فعلية تعزل الشبكات الأمنية تماما عن العالم الخارجي. وبالتالي تُفصل الأنظمة المتطورة عن الأنظمة الأمنية البدائية لحمايتها من البرامج الضارة أو خرق البيانات. وعلى الرغم من ذلك، لا تقدم الفجوات الهوائية سوى حل بدائي من خلال التخلص من المخاطر دون تسهيل استخدام الشبكة. ونظرًا لعزل الشبكة الكامل، يتعذر نقل المعلومات أو البيانات في الوقت الفعلي عبر القناة. [16]

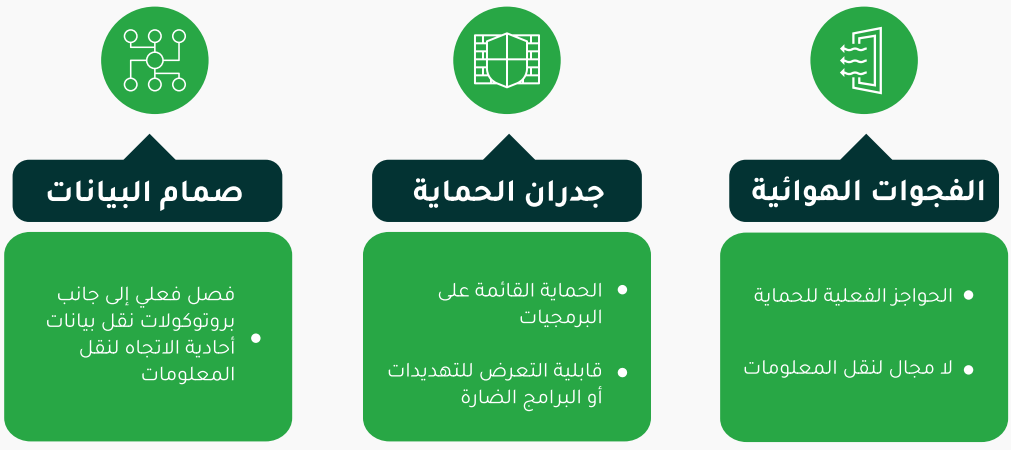
- **يستخدم أقل من 10% من أنظمة التحكم الصناعية الفجوات الهوائية للتحكم في الأمن السيبراني. [5]**

تتبع جدران الحماية الاتجاه النفعي من خلال إدارة مجموعة من الشبكات المتنوعة عبر بروتوكولات الاتصالات التي تعتمد على البرمجيات. ومن الناحية النظرية، تقدم جدران الحماية قناة آمنة لتبادل البيانات ونقل المعلومات. وعلى الرغم من ذلك فإن إعداد برمجياتها يعرضه لعدد من نقاط الضعف في شكل هجمات الباب الخلفي والأخطاء البرمجية والتثبيت الخاطئ

- **يرى 36% من الفرق الأمنية أن عدم الدقة وأخطاء إعدادات جدران الحماية تؤدي إلى زيادة مدة إعادة العمل. [7]**

ويؤدي صمام البيانات إلى تحسين شبكات الأمن الإلكتروني من خلال ضمان النقل الآمن للبيانات والمعلومات. وللتغلب على قيود الفجوات الهوائية وجدران الحماية، يعمل صمام البيانات على فصل الأجهزة لحماية الشبكات بالإضافة إلى استخدام اتصال أحادي الاتجاه لنقل المعلومات

- **ولم يتم الإبلاغ عن أي حالة خرق للبيانات أو تجاوز في صمام البيانات لأنه آمن بنسبة 100%.[15]**



خاتمة

تقوم المؤسسات بتطوير تقنيات جديدة وتبنيها لمشاركة المعلومات القيمة في عالم مترابط. وبالتوازي مع ذلك، تتطور بيئة تهديدات شبكات الأعمال والمعلومات أيضًا من حيث الحجم والتعقيد. ولا تكفي الحلول الأمنية القياسية لتفادي التهديدات السيبرانية متعددة الأشكال. وتوجد حاجة ملحة لبرامج الأمن السيبراني المرنة التي تتكون من تدابير مختلفة لتحسين الوضع الأمني .

وتتمثل أحد هذه الأساليب الاستباقية المرنة في استخدام جدران الحماية وصمام البيانات معًا. ومن المحتمل أن تكون جدران الحماية جزء لا يمكن الاستغناء عنه من أمن الشبكة. وعلى الجانب الآخر، يتغلب صمام البيانات على الفجوة في القدرات ويقدم شبكة أكثر موثوقية ولا يمكن قرصنتها. وتمتلك كل منها نقاط القوة الخاصة بها وتعتبر مناسبة نوعًا ما في بيئات وظروف مختلفة. وفي الآونة الأخيرة، أدت زيادة تعرض جدران الحماية القائمة على البرمجيات للهجمات الخارجية إلى تسليط الضوء على صمام البيانات في مجال الأمن السيبراني. وبعد أن أصبحت الهجمات أكثر احتيالًا، فإن استخدام أدوات مختلفة للعمل بشكل متناسق هي أفضل طريقة لمنع الهجمات السيبرانية وتقليل الخسارة الناجمة عنها .

وتركز رؤية 2030 للمملكة العربية السعودية على بناء بنية تحتية رقمية متطورة للأنشطة الصناعية المتقدمة مع تسهيل توطين التصنيع والبحث والتطوير والخدمات الأخرى. وقد نوعت شركة الإلكترونيات المتقدمة عروضها وفقًا لهذه الرؤية. ويعتبر صمام البيانات أحد المنتجات التي تدعم رحلة التحول الرقمي التي تقوم بها المملكة العربية السعودية من خلال حماية شبكات المعلومات من التهديدات الخارجية. ونظرًا لما له من خواص أساسية، يقدم صمام البيانات فرصة يجعلها ذات أهمية بالغة في الأمن السيبراني .

المراجع

1. Cybercrime Magazine. 2019. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. [online] Available at: <https://cybersecurityventures.com/cybersecurity-almanac-2019/>

2. Upguard.com. 2020. Why Is Cybersecurity Important?. [online] Available at: <https://www.upguard.com/blog/cybersecurity-important>

3. Naseba. 2020. Companies In The Middle East Highly Vulnerable To Cyber Attacks, Says Pwc Study - Naseba. [online] Available at: <https://naseba.com/content-hub/topic/cyber-security-topic/companies-middle-east-highly-vulnerable-cyber-attacks-says-pwc-study/>

4. Arab News. 2020. Aramco, AEC To Develop Kingdom'S First Data Diode. [online] Available at: <https://www.arabnews.com/node/1635101/corporate-news>

5. The Hague Security Delta 2019. Understanding the Strategic and Technical Significance of Technology for Security The Case of Data Diodes for Cybersecurity [ebook] Available at: <https://www.thehaguesecuritydelta.com/media/com_hsd/report/246/document/HSD-Rapport-Data-Diodes.pdf>

6. Web.mit.edu. 2020. [online] Available at: <http://web.mit.edu/ha22286/www/papers/CSIIRW10.pdf>

7. https://www.firemon.com/state-of-the-firewall-report-2019/. 2019. State Of The Firewall. [online] Available at: <https://3hggz2ft-dz41fqjfc37yqew1-wpengine.netdna-ssl.com/wp-content/uploads/2019-FireMon-State-of-the-Firewall-Report.pdf>

8. Arab News. 2020. Cyberattacks Hit 95% Of Saudi Businesses Last Year, Says Study. [online] Available at: <https://www.arabnews.com/node/1718596/saudi-arabia>

9. HostingTribunal. 2020. 40 Scary Hacking Statistics That Concern Us All In 2020. [online] Available at: <https://hostingtribunal.com/blog/hacking-statistics/#gref>

10. Sans.org. 2015. SANS Institute: Reading Room - Firewalls & Perimeter Protection. [online] Available at: <https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057>

11. Watchguard.com. 2020. Positioning Your Firewall. [online] Available at: <http://www.watchguard.com/training/fireware/82/archite8.htm>

12. ROI4CIO. 2020. Data Diode Review, Comparison, Best Products, Implementations, Suppliers. | ROI4CIO. [online] Available at: <https://roi4cio.com/en/categories/category/data-diode/>

13. FireMon. 2017. Misconfigurations: The Firewalls Greatest Threat - Firemon. [online] Available at: <https://www.firemon.com/misconfigurations-firewalls-greatest-threat/>

14. Netsparker.com. 2017. Vulnerable Web Applications On Developers, Computers Allow Hackers To Bypass Corporate Firewalls. [online] Available at: <https://www.netsparker.com/blog/web-security/vulnerable-web-applications-developers-target/>

15. PCMag India. 2018. Black Hat Researcher Shows Why Air Gaps Won't Protect Your Data. [online] Available at: <https://in.pcmag.com/news/124706/black-hat-researcher-shows-why-air-gaps-wont-protect-your-data>

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

شركة الإلكترونيات المتقدمة

مطار الملك خالد. المنطقة الصناعية

P.O.BOX 90916,

الرياض 11623 , المملكة العربية السعودية

Email - info@aecl.com +966112201350

/AECSaudiArabia