senseye

White Paper

Security Considerations for Scalable Predictive Maintenance

Introduction

Predictive Maintenance and other connected technologies associated with the smart factory revolution offer huge opportunities for production efficiency and visibility, but they also bring an additional operational risk – security.

Cyber-attacks are increasing and the manufacturing sector is being hit with data theft, ransoms for access to locked data, machinery downtime, site safety, and build quality threats. Here we look at the security considerations organizations should be taking note of when implementing a scalable Predictive Maintenance program.

What is predictive maintenance?

Predictive Maintenance brings together sensor data, machinery build information and environmental factors, using analysis and data modelling to identify maintenance issues before they become problems. By maintaining equipment before it shows outward signs of failure or causes unplanned downtime, organizations can boost profitability and throughput while spending less through a proactive, rather than preventative, approach to maintenance.

The importance of security

November 2019 Pilz, one of the world's largest producers of automation tools, suffered a ransomware infection which impacted all its locations across 76 countries for more than a week.[1]

July 2018 A hacker put an airport's security system access onto the dark web for sale for just $10.[2]

March 2018 The city of Atlanta was hit by a ransomware attack, holding its online services to ransom for $55,000 in bitcoin. It is reported that the city spent over $2.5 million recovering from the attack.[3]

June 2017 Ransomware hit Cadbury's in Australia, after disrupting Evraz and Rosneft steel and oil firms in Russia.[4] The same month, Honda was forced to halt production in one of its factories in Japan after finding WannaCry malware across its international networks, including Japan, North America, Europe and China.[5]

May 2017 The NHS in the UK was crippled by the WannaCry ransomware, which locked access to files until a ransom was paid. The same ransomware quickly went on to attack several more factories around the world.[6]

Clearly, security cannot be ignored, but it should also not be reason to halt innovation. Within the manufacturing sector, there is huge opportunity in the use of technology to streamline production for cost savings, increased quality and visibility from start to finish. So, what can be done to minimize the risk of cyberattacks?

1. https://www.zdnet.com/article/major-german-manufacturer-still-down-a-week-after-getting-hit-by-ransomware
2. https://www.mcafee.com/blogs/consumer/consumer-threat-notices/airport-security-system-dark-web-rdp-shop
3. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare
4. https://www.theguardian.com/technology/2017/jun/28/petya-cyber-attack-cadbury-chocolate-factory-in-hobart-hit-by-ransomware
5. https://www.forbes.com/sites/peterlyon/2017/06/22/cyber-attack-at-honda-stops-production-after-wannacry-worm-strikes
6. https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

senseye

Security considerations

Continuous improvement

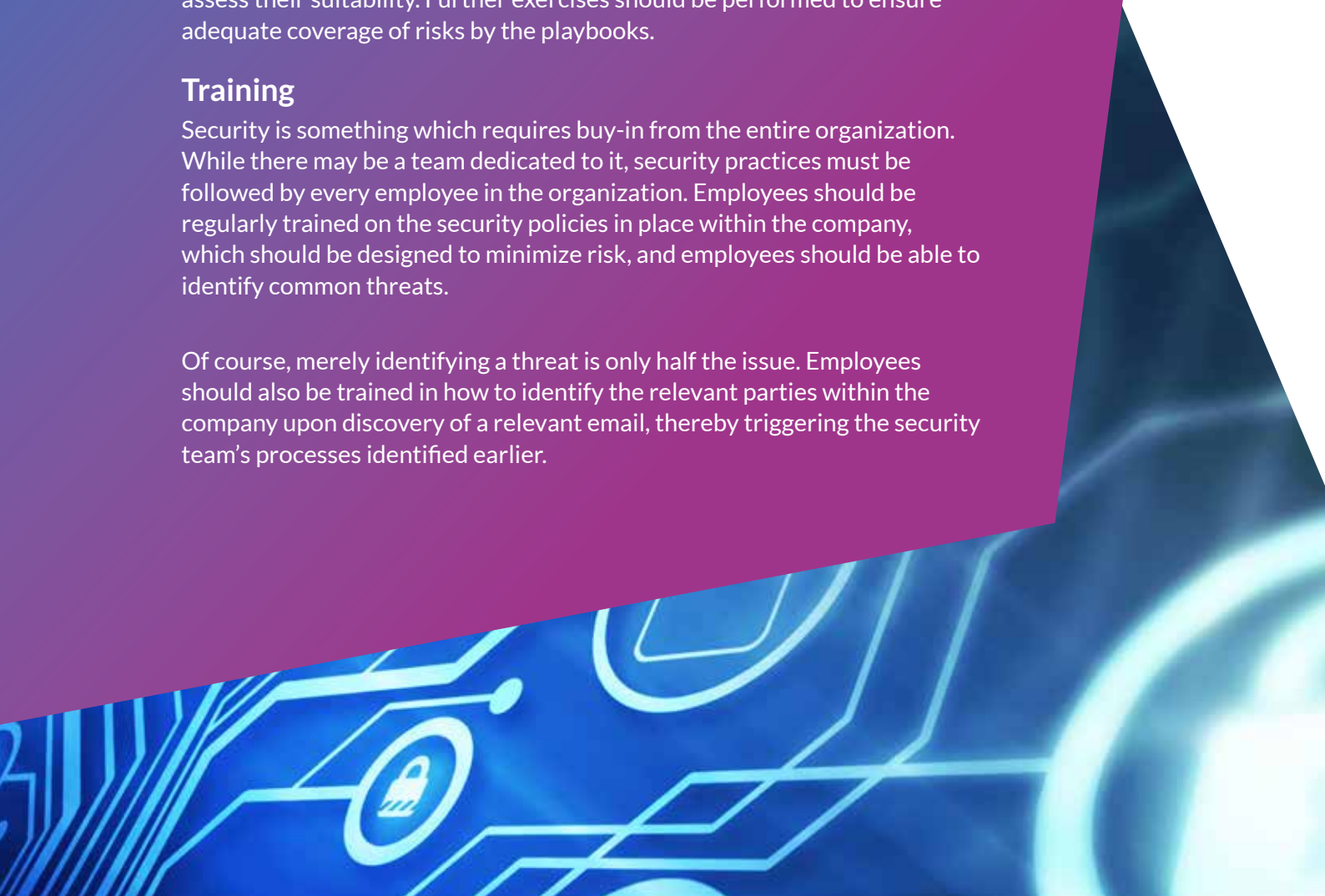
Simply implementing a firewall or security patch doesn't halt cybercrime and as a result, security is a continuous process. New vulnerabilities are being discovered constantly, and hackers often use automated tools to scan cloud-facing networks for known vulnerabilities. Frequently they will be looking for issues that are known by the community, and for which security patches are available but have not yet been applied by administrators Consequently, it is important to monitor the latest information on vulnerabilities and breaches relevant to your organization, its tools and infrastructure, and to ensure that your systems are kept up to date.

No matter how vigilant the organization, there is an ever-present risk of a security incident, and the organization must be prepared to handle such a situation. An in-house security team should be in place to ensure that security is regularly assessed, and they should have in place policies and playbooks for how to handle various incidents that may occur. These should include steps to, contain the issue, gather any relevant evidence, resolve, recover and of course review the company's response paying attention to lessons learned. Depending on the nature of the incident and the data that was exposed (if any), third parties such as the information commissioner may need to be notified. Regular exercises should be performed in which an incident is simulated, and response teams run through the playbooks to assess their suitability. Further exercises should be performed to ensure adequate coverage of risks by the playbooks.

Training

Security is something which requires buy-in from the entire organization. While there may be a team dedicated to it, security practices must be followed by every employee in the organization. Employees should be regularly trained on the security policies in place within the company, which should be designed to minimize risk, and employees should be able to identify common threats.

Of course, merely identifying a threat is only half the issue. Employees should also be trained in how to identify the relevant parties within the company upon discovery of a relevant email, thereby triggering the security team's processes identified earlier.



Continuous monitoring

The monitoring tools on an organization's systems are its eyes and ears. It is important to pay close attention to activity in order to establish a baseline against which suspicious behavior can be detected. Inbound and outbound network activity, service requests, user activity and server load may all be useful sources of data in this regard. Furthermore, in the event of an incident, logs will form a crucial part of the investigation performed by the organization's security response team.

As well as network activity, other internal sources such as configuration changes should be monitored. Often a breach occurs due to nothing more than accidental misconfiguration of a service, as was the case in the recent Virgin Media incident, amongst countless others. Indeed, sometimes the issue is that the default configuration from a vendor is weak and has not been changed (the classic example being the use of default passwords). Having a robust change-management process will help in this regard, as well as performing regular internal audits, but it is also important to have specialist third parties perform regular audits of your systems to find any issues that may have been missed internally.

Third party auditing

Best practice dictates that independent third parties are used for regular external security audits, at least annually or upon any significant change to your infrastructure. Using independent security experts enables solution providers to proactively identify any potential vulnerabilities, so they can quickly mitigate any potential risks or concerns and keep in pace with the ever-changing cybersecurity environment. These activities should include security audits and rigorous vulnerability scans and penetration testing to ensure the protection being offered by the solution meets industry expectations.

All Predictive Maintenance vendors should be able to supply security documentation, answer any questions and provide IT teams with the information they need. Industrial and office computers are internal. Ensuring staff are mindful of security, updating passwords, ensuring antivirus software is up to date, encrypting data, keeping on top of permissions, maintaining a firewall; these are some of the areas which are critical in maintaining a secure network. However, any addition to a network carries additional risk and needs to be properly assessed.

SECURITY CHECKLIST

1. Assess the risk

Risk assessments are essential when bringing a new piece of technology into a business and should include all touchpoints, passwords, staff access, the movement of data, supplier security, etc.

2. Design from the outset with usable security in mind

Security is much easier to implement when it has been considered from the start. Ideally, it should be as transparent as possible to the users – if it's doing its job correctly, it won't be noticed, and if it gets in the way, users will find an easier path.

3. Choose the right supplier for your business

It is critical to have confidence in the supplier and their product. Full system information including security should be available and any concerns or requests should be dealt with efficiently and intelligently. Look for accreditations such as ISO27001 and ISO9001 that show the company has robust information security and quality policies in place.

4. Ensure good encryption

At a minimum, whenever data is transmitted over the cloud, it should be encrypted. Current industry standards recommend TLS1.2 as a cryptographic protocol, and AES-based cipher suites. At rest, sensitive data should also be encrypted, with AES-256 being the current industry recommended algorithm.

5. Keep it simple

Always look for the 'least exposure' option. Use firewalls to limit communication between hosts, and to minimize your exposure to external networks. Many companies also separate operational machinery from internal IT networks. Always ask if less contact is possible; this can always be increased over time as confidence grows and opportunities are realized.

6. Consider the potential of the project

The potential opportunity of a project is only there with a degree of freedom and lack of restrictions. While security is critical, it is a balance, and there's no reason for it to cripple innovation.

7. Create an incident management plan

If an incident does happen, it is important that everyone knows how to respond so the threat can be quickly contained and managed to minimize the impact

8. Continually review security

Security isn't a one-off job. The threat landscape and best-practice recommendations are always changing. Your security approach must be adaptable and nimble.

Security with Senseye

Senseye is an ISO27001 accredited company and takes data security seriously. Data stored within Senseye is encrypted at rest, and in transport in line with industry-recommended standards.

Senseye PdM is regularly tested and audited by independent security organizations, and in addition, all employees adhere to a set of strict internal security policies covering a range of topics such as data handling, use of equipment and software development to ensure that confidential client data is treated with the appropriate safety and care. Senseye believes in transparency and makes available all results and reports to clients.

Online Sources

For all companies, especially those starting to develop an information security process, sources such as the National Cyber Security Centre (ncsc.gov.uk) and the National Institute of Standards and Technology (nist.gov/cybersecurity) contain a wealth of invaluable information.

Conclusion

Security is a major concern for any business, and it is crucial to put in place a thorough and robust security strategy to minimize the risk of a cyber-attack. However, when a cloud-based Predictive Maintenance solution is designed with security in mind it can be safer than having some third-party software installed inside the network.

Getting full commitment from all stakeholders, internal and external, to ensure continuous improvement, ongoing network monitoring, transparency regarding solution providers' security arrangements and protecting network access means that risk can be balanced with innovation and opportunity.

senseye

ABOUT THE AUTHOR

Dr. Harry Rose is the Security Lead at Senseye. After Graduating with a PhD in Computer Science, Harry spent his early career working on various "smart" devices and HUMS data software projects.

Having joined Senseye in 2015, Harry has been heavily involved in the back-end development of Senseye PdM, and now leads the company's security efforts, overseeing all accreditations and policies.

About Senseye

Trusted by Fortune 500 industrial companies, Senseye's technology solutions suite, Senseye PdM, is used to monitor more than 20,000 industrial assets in real time around the world. Senseye PdM forecasts machine failure and remaining useful life of industrial assets automatically, enabling users to guarantee uptime and asset availability, streamline production processes and ensure safer, more efficient operations. Senseye PdM can be deployed at scale within 14 days and, used alongside Senseye's methodologies, typically delivers a complete Return on Investment within three months of adoption.

To start your Predictive Maintenance journey with our experts and see our solutions live, click here to request a demo or get in touch with our team.

UK (HQ)
Epsilon House
Enterprise Road
Southampton Science Park
Southampton
SO16 7NS
United Kingdom

+44 (0) 845 838 8615

UK
90 Long Acre
Covent Garden
London
WC2E 9RZ
United Kingdom

+44 (0) 845 838 8615

USA
100 Madison Street
Unit 308
Nashville
Tennessee
37208
USA

+1 415 523 0447

Please visit our website to see the contact details of our other office locations.

sales@senseye.io

Follow us: