tion or IoT device contains more than 500 components. While many of these components are selected by a developer, many are brought in automatically by a repository manager such as Maven or Yocto.

These top-level components and their dependencies are the most common items tracked and managed by the teams, but other components are used as well. The next most common components are monolithic source trees copied into the codebase. This is typically how a library like OpenSSL or zlib is downloaded and introduced into a codebase. These are often found through visual inspection, or by grepping or searching for licence files, readme files, known filenames or known embedded strings. Other forms of component use include source code coming from forums or tutorial sites. Components at this level should eventually be tracked as well. Components in both source and binary forms should be reviewed and those with binary forms should be examined to confirm if the source code used to produce them is available.

The software supply chain

Often, code coming from outside sources is accepted into the codebase with little question or review – especially if it is coming from a commercial vendor. It is important for developers to have as high expectations for the code they bring in from others, as the code they write themselves. If they are not receiving a bill of materials with the code, this should be treated like a software defect.

There are a couple of ways that companies are building this awareness into their procurement process. The first is to insert contract language that details the expectations around disclosure of third-party components, as well as the process for receiving notice of patches or upgrades related to third-party vulnerabilities. Additionally, development teams are using targeted analysis for source and binary materials looking for undisclosed content. Typically, two or three undisclosed components, especially if they have either reported vulnerabilities or licence issues, are enough to open a dialogue with the outside software vendor.

This conversation regarding the undisclosed components is used to stress the importance of receiving the full bill of materials and also shows that the company is watching out for its interests. Vendors that are not able to deliver the expected level of disclosure should not be used for future work. The philosophy of 'it was safe when we shipped it' is no longer sufficient, especially if the code is ending up in devices with full-time network connections and little monitoring. The sooner a vendor can raise the alarm, the sooner a tested upgrade can be pushed to the devices and installed base.

Pulling it all together

By changing attitudes about who is responsible for security around third-party component usage, educating teams about what can be done to discover, manage and remediate issues involving these components, as well as holding vendors and suppliers to the same level of expectations, modern software developers can build in security in an environment where half of the code they use was written by someone outside their organisation.

About the author

Jeff Luszcz is a VP of product management at Flexera Software (www.flexerasoftware.com). Previously, he was founder and CTO of Palamida. He has helped software companies use open source software while complying with licence obligations and keeping on top of security issues. Throughout his career, he has been active in the Java, Macintosh and open source software communities. Luszcz is also the author of several well-known Macintosh software utilities and has served as a technical editor for Wrox Press.

References

1. Spring, Tom. 'Bashlite family of malware infects 1 million IoT devices'. ThreatPost, 30 Aug 2016. Accessed Aug 2017. https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/.
2. 'Shellshock (software bug)'. Wikipedia. Accessed Aug 2017. https://en.wikipedia.org/wiki/Shellshock_(software_bug).
3. The Heartbleed Bug, home page. Accessed Aug 2017. http://heartbleed.com/.

Healthcare and digital transformation

Eileen Haggerty, Netscout

Eileen Haggerty

As with most other industries, healthcare has seen significant benefits from digital transformation (DX), with the adoption of new technologies helping to deliver secure, high-quality patient care and drive greater business efficiency. Electronic health records (EHR), digital imaging, e-prescription services and enterprise resource planning systems are among the digital services that have been integrated into the extensive IT systems of many healthcare organisations.

The healthcare sector has also seen the impact of the burgeoning Internet of Things (IoT), with the adoption of connected devices becoming more widespread as technologies and connectivity improve. The global healthcare sector will invest almost $410bn in an IoT market comprising medical devices – including wearables, as well as implantable and stationary devices – systems,

software and services, according to a report by Grand Research Review.[1]

The value of data

Global industries have experienced a shift in the past decade, with the value of data and digital services growing, and said digital services, applications and software increasingly being relied upon to drive new business models and growth. The healthcare industry is no exception. Continuous, secure access to patient data for medical professionals has become a necessity over recent years for safe, prompt and efficient treatment. Patient record applications (Electronic Health Records, EHR) and subsequent databases of information are implemented and maintained by healthcare IT organisations in on-premise datacentres or in the cloud. This data includes medical records and images, doctor's notes, test results, e-prescriptions, insurance claims and policies, as well as the huge volumes of information generated by IoT devices.

The business of healthcare has changed as a result. In this current environment, healthcare providers have more access to patient data (both historic and real-time) and applications than ever before, which absolutely helps to provide a safer, more consistent care service. However, the increased complexity of the IT networks that power today's healthcare organisations, as well as the sheer volume of data traversing these, has added to the challenge of ensuring network and data security.

According to Accenture, one in eight UK consumers has had personal medical information stolen from technology systems. Furthermore, it is not clear whether the original data holders (cited as pharmacies, hospitals, urgent care clinics, doctor's offices and retail clinics) were aware of these security breaches, as more than one-third of the consumers found out about the breach themselves or learned about it through noting an error on their health record or credit card statement.[2] This highlights both the insecurity of healthcare IT networks and the potential lack of insight and visibility that those overseeing these networks actually have.

The recent WannaCry ransomware attack also illustrated the devastating impact that cyber-security breaches can have on the healthcare sector. Although UK government officials have suggested that no patient data was lost, the fallout of the attack will have severely affected the sector's ability to deliver adequate care and – more importantly – patients' ability to access it. Some 45 NHS sites were hit across the UK, resulting in issues such as delayed or cancelled appointments and procedures and compromised or no access to medical records: x-ray and doctor alert systems were also affected.

"The increased complexity of the IT networks that power today's healthcare organisations, as well as the sheer volume of data traversing these, has added the challenge of ensuring network and data security"

Data breaches such as these are a universal issue and no healthcare organisation is immune. In March 2017, for example, a data breach incident was reported to the US Department for Health and Human Services (HHS) involving 697,800 patient records.[3] In other industries, cyber-security breaches may result in transactions being cancelled or delays, or loss of personal data; but in the healthcare sector, the impacts and losses are potentially far more devastating.

Safeguarding data

Securing and monitoring networks should be a priority for healthcare IT professionals. Yet this is a complex task, with next-generation technologies being introduced and legacy systems often requiring ongoing updates in an attempt to improve the overall efficiency, speed and security of networks. Compounding the complexity of this environment are the ongoing developments in software-defined datacentres, network virtualisation, cloud and mobility. These factors all drive the need for real-time service assurance monitoring by all parties across the spectrum of the healthcare industry.

The need to safeguard data is not only essential to ensuring operational and service efficiency, in many countries it is also required by law. In the UK, healthcare data needs to be compliant with the Data Protection Act. This includes the requirement that 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'.[4]

Taking a proactive approach and ensuring end-to-end network visibility to detect and identify anomalies must therefore form a vital part of the cyber-security and business assurance strategy of all healthcare organisations.

EU member states will have to adhere to similar guidelines when the EU General Data Protection Regulation (GDPR) enters into force and, by 6 May 2018, must be transposed into national laws of countries in the EU. Consumers in the EU already benefit from the right to state-provided healthcare access while travelling in member states using a European Health Insurance Card. By standardising data protection across the EU, the updated regulation should ease access and transfer of data across borders, as well as strengthening data security.

In addition to guaranteeing the security and interoperability of different technologies, continuous monitoring of EHR applications is also essential for healthcare providers. The ability to assess performance metrics and EHR transactions status activity, such as response time analysis, is crucial for successful clinical practice and healthcare services and is also a regulatory requirement in some countries. In the US, for example, the Health Information Technology for Economic and Clinical Health (HITECH) Act can dictate penalties for healthcare organisations that do not implement EHRs. Similarly, the ineffective protection of patient data can also mean high penalties for healthcare organisations. Violations of the Health and Insurance Portability Act (HIPAA), passed in 1996, can be significant. Fines per violation can reach $50,000, though