Microsoft

Secure Software Development Trends in the Oil & Gas Sectors

How the Microsoft Security Development Lifecycle helps protect critical industries

Secure Software Development Trends in the Oil & Gas Sectors

Microsoft

Table of contents

Microsoft

Introduction

The global oil and gas industry is one of the world's largest in terms of sheer dollar value. But size does not guarantee protection in an age when large corporations can lose millions of dollars in sensitive data – or worse, control over parts of their networks – by simply opening a malicious email attachment.

Despite the tens of billions of dollars of assets at stake, major portions of this industry remain vulnerable to cyberattacks, ranging from state-sponsored corporate espionage to so-called "hacktivists" seeking to make political statements through their choice of target.

The industry's troubles have attracted considerable attention to the normally opaque world of cybersecurity. In May 2012, the U.S. Department of Homeland Security confirmed an ongoing campaign of attacks from state-sponsored actors against oil pipeline companies extending through the first half of that year.

Companies' systems were invaded and proprietary information was stolen. In July 2012, Wired magazine reported that the "hacktivist" group Anonymous published some 1,000 email addresses for accounts belonging to energy firms, as well as hashed and unencrypted passwords. And in August 2012, a limited number of oil & gas companies in the Gulf region were put on the front page following an apparent spate of Trojan malware infections.

In this evolving threat landscape, companies can easily find themselves outgunned, said Paul Williams, executive director of security services at White Badger Group, who has experience advising clients in the oil and gas industry.

"When you're talking about economic espionage from a foreign intelligence agency, it might be thousands attacking forty guys who know what they're doing on defense side," Williams said.

A Holistic Approach

In the face of these daunting security challenges, industry leaders, outside security analysts, consultants and software experts have been calling for a comprehensive approach to cybersecurity in the oil and gas industry. Their message: given the nature of the threats, companies must instill a bottom-up, company-wide security culture. This includes procedures and policies to let all firms in the sprawling, decentralized industry respond to and defend against agile enemies, because any weak link in the overall supply chain can be a significant problem.

"Security is everybody's responsibility in the company," said Aaron Merrick, vice president of information technology at Apache Corporation, a multinational oil and gas company based in Houston with more than 3 billion barrels' equivalent of proven oil and natural gas reserves.

"I don't want people on the network thinking, 'Oh that's somebody else's job,'" he said. "It's everybody's job because it can't be done without the participation and cooperation of everybody in the company that has access."

At the same time, the oil and gas industry has unique needs that set it apart from other infrastructure, such as the nuclear power industry, where regulation is much tighter and protocols are more closed.

"In oil and gas the culture is very open. You have a lot more work done by consultants, vendors and suppliers," said Jonathan Pollet, founder and principal of Red Tiger Security, a data security consultancy with extensive experience in the oil and gas industry. "The question is how do you allow business systems to function while keeping them secure from people who shouldn't have access to them?"

As companies in the oil and gas industry move to address their specific security concerns, they are looking for holistic frameworks that will help them to implement prescriptive process changes. Several are discovering that an existing security development process created by Microsoft called the Security Development Lifecycle can help to address not only software security, but also broader infrastructure design.

Known as the SDL, the Security Development Lifecycle is a step-by-step process that helps companies incorporate security into applications from conception to release and beyond.

This approach is used in companies of every size and in every industry, from small software development firms to global enterprises. It's also free. Microsoft provides the SDL to customers and competitors alike under the theory that everyone wins in a more secure environment. The basics of the SDL are relatively easy to introduce, even to those with no specific security experience. The Simplified SDL is a very accessible document designed to help managers create a long-term framework for creating secure software.[1] At 17 pages the document is designed to be a practical and actionable introduction to secure software development.

A comprehensive process like the SDL helps build practical solutions out of the belief that cybersecurity is every employee's job, from the CEO on down. The SDL is general enough that it can be adapted to a wide range of security environments, but rigorous enough to meet exacting standards in the most security-sensitive industries.

SDL CORE STEPS

At its core, the SDL encompasses several basic steps, including:

- Training, plus setting secure development education requirements for all employees.
- Setting minimum standards for security.
- Setting minimum standards for privacy.
- Threat modeling.
- Using lessons learned during threat modeling to update product design specifications.
- Using secure coding practices to reduce common security errors and mitigate the effects of errors that remain.
- Testing to validate the effectiveness of secure coding practices.
- Performing a final security review.
- Creating a security response plan in case a vulnerability is discovered.
- Performing an analysis to understand the cause of any vulnerabilities.

[1] http://www.microsoft.com/en-us/download/details.aspx?id=12379

Microsoft

Solutions for a Diverse Global Industry

The oil and gas industry is a very diverse global industry that must operate in extreme conditions. Exploration, production, processing and delivery of products require enterprises to work with many different external partners and third parties. Increasingly, oil and gas companies are becoming integrators for a wide range of services and technologies they purchase to help them deliver their final product, said Alan Hasling, an account technology strategist for Microsoft who works with the oil and gas industry.

Hasling cites the example of the compression process used to pressurize and transport natural gas. In previous years, a company might have bought a gas compressor and done the job in-house, but companies now are more likely to purchase a compression service, Hasling said.

"We write very little software," Merrick said of Apache Corporation. "We purchase and implement tools that help Apache employees get their job done."

This makes security an especially tricky business, as very few companies have complete control over the application lifecycle, Pollet said.

Therefore, building transparency into security processes is a challenge.

"It's very difficult to convince all these vendors to standardize on a solution," Pollet said. He explained that companies tend to develop unique approaches to security. That makes it tricky for best practices to flow through such a large infrastructure, which can make each company more vulnerable rather than less.

"It only takes one weak link in the chain to take down the system," he said

But the SDL can help analyze security practices used to develop critical software systems in this decentralized environment. Information about security processes, such as the SDL, should be an important part of any security discussion a company has with a vendor in its supply chain.

Some firms are already adopting this process-based approach. Different tenets of the SDL are finding their way into the oil and gas industry as companies take a more holistic approach to security. Some companies don't use the SDL in its entirety, but what they are doing in many ways mirrors the overall goals of the SDL – and incremental application of SDL processes leads to incremental improvements in security. It's not an all or nothing equation.

Apache Corporation uses a modified security framework that considers everything from physical to logical access to application security to data protection to data continuity, Merrick said. The company also expects its key suppliers to address security concerns in a logical, holistic manner.

The bottom line: Accountability is a key component of security at Apache.

The SDL Approach Pays Dividends

The SDL is particularly relevant as oil and gas companies work toward better application security and security of the outsourced applications they use. Companies in the industry have traditionally responded to cyberattacks by patching and updating their operational infrastructure. But that's not enough to create a secure environment. Increasingly, the applications companies use to conduct day-to-day business and control business processes in the field are becoming the major points of attack because that is where valuable data is stored.

The trouble is that while many inside the industry argue that the oil and gas business takes cybersecurity seriously, a sprawling network of players within this global industry — all with different interests and different roles — implement their own solutions and standards for application security.

The industry is recognizing the usefulness of a process framework like the SDL for helping to prioritize risk and guide secure development of applications. One of the key constructs of the SDL is threat modeling, which helps prioritize mitigations and resources. This concept is now being looked at broadly in the industry.

SDL LEADS TO REAL COST SAVINGS

A 2011 study by the research firm Aberdeen Group found that companies that incorporate security throughout the development process, rather than wait until the end of the process to perform reviews and tests, made **four times the return** on their annual investments in application security.

$8.4 MILLION

is the average estimated cost per 24 hours of downtime due to cyberattacks in the oil and gas industry

The average cost of remediating an application security-related vulnerability:

$300k PER INCIDENT

"I believe we shouldn't even approve a project without doing threat modeling first," said one security executive from a major oil field services company who requested anonymity due to the sensitive nature of the strategic infrastructure the executive supervises. "If there is a project, security should be part of the project lifecycle; that is very clear."

"I still see a lot of projects where security is an afterthought," the executive said. "People need to understand that security needs to be part of the process from the beginning."

Despite the challenges, it's crucial – and possible – for oil and gas companies and their suppliers to adopt a structured approach to application security. The SDL – which guides developers to build in security before a single line of code is written – can help them improve security in this key area and to provide needed transparency and standardization.

One of the SDL's strengths is that it is a process-based approach that is flexible and designed to be incorporated into any organization's product lifecycle – even outside the software industry. The SDL has been successfully adapted and deployed at infrastructure companies such as Iowa-based MidAmerican Energy Co. and at Itron, a global technology company and builder of smart grid electricity and water meters based in Liberty Lake, Washington.

At MidAmerican, executives held company-wide SDL training in response to attacks on company websites. Not only did the SDL-inspired security approach reduce the impact of attempted attacks, it also increased efficiency, including a 20 percent productivity gain resulting from less change during testing and fewer after-the-fact fixes to code.

Itron, a company with explicit parallels to the oil and gas industry, adapted its utility meters – meant to live in the field for decades – to a rapidly changing cybersecurity environment. Its engineers adapted the SDL to the design of the smart meter, from how to prevent it from being broken into physically – securing seals and closures – to how to protect its electrical systems and software.

A secure product isn't the only benefit – the SDL has also led to real cost savings. A 2011 study by the research firm Aberdeen Group found that companies that incorporate security throughout the development process, rather than wait until the end of the process to perform reviews and tests, made four times the return on their annual investments in application security. The same study estimates that the average cost of remediating an application security-related vulnerability is around $300,000 per incident, but the average annual investment developers make in deploying a comprehensive approach to application security – including people, processes and training – totals about $400,000.

And according to a 2011 study by security firm McAfee, the cost per 24 hours of downtime due to cyberattacks is highest for oil and gas companies, with an average estimate of $8.4 million per day lost.

Pollet said there are practical steps he would advise any company to take in order to make itself more secure. In many ways, his suggestions mirror the SDL in that he advises companies to address the highest risks up front.

First off, he said companies must identify key assets and then do threat modeling on how to protect those assets. Examples might include doing secure application development differently or dividing their network control assets into different sectors so breaches can be localized. Companies must also determine how they securely manage outside access to their data systems and, after their systems are protected, how they will be continuously monitored.

This kind of integrated, disciplined approach to security needs to be built, Pollet said, into the basics of system architecture and development practices. That includes access to secure infrastructure, rudimentary network security and the updating of software.

The next obvious steps are integrating these basic procedures into more sophisticated software security challenges, Pollet said, which include managing access to directories, developing strong passwords and, finally, securing the actual deployed applications through better development practices.

"As a security provider," he said, "these things are a no-brainer."

Looking Forward

Challenges remain, and security experts stress that oil and gas companies are only beginning to grapple with the need for end-to-end security as part of their corporate culture. Companies need to remain vigilant, because attackers' capabilities are increasing all the time.

Merrick foresees oil and gas companies will become more cognizant of the need for end-to-end security. That includes more cooperation and standardization across the industry, with the possibility of federated authentication systems to help companies know what is safe and what is not when transferring data.

But ultimately, Merrick believes security is an iterative process that will continue to rely on time-tested security skills such as the ability to locate and address dangers and to learn from security breaches if they do occur.

In Merrick's mind, effective security means identifying real threats amidst the buzz and the hype. He cites one prominent example in Illinois, where a pump failure at a water plant in 2011, first reported to be caused by hackers, was later revealed to be a false alarm.

"You have to be able to sort through the hype from what's going on day-to-day," he said. "But you can never be satisfied that you know everything or that will be your Achilles heel. Anything out there that has been exploited is just teaching us the lesson that we don't know what will be exploited in the future."

The SDL is one tool companies are using to meet the dual challenges of security: addressing known threats while staying flexible enough to respond to the unknown.

"…YOU CAN NEVER BE SATISFIED THAT YOU KNOW EVERYTHING OR THAT WILL BE YOUR ACHILLES HEEL. ANYTHING OUT THERE THAT HAS BEEN EXPLOITED IS JUST TEACHING US THE LESSON THAT WE DON'T KNOW WHAT WILL BE EXPLOITED IN THE FUTURE."

– Aaron Merrick, vice president of information technology at Apache Corporation