April 2017 ibmsystemsmag.com

POWER SYSTEMS

IBM Systems

Private, Public, Hybrid?

That is the Question

IBM Power Systems is Your

CLOUD ANSWER

PAGE 18

Chilewich Sultan patterns a new DR solution

PAGE 14

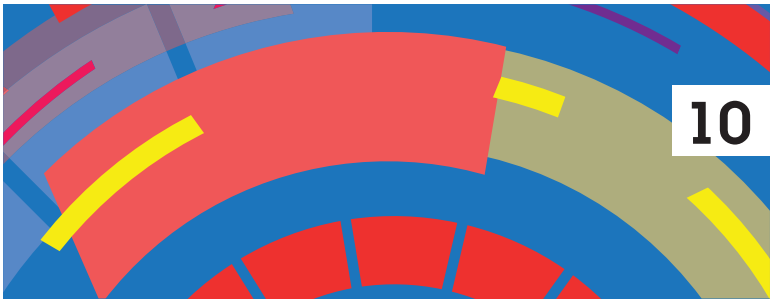
New tool buys time for cybersecurity

PAGE 25

INSIDE

APRIL 2017

Cover illustration by Andy Potts



FEATURES

DEPARTMENTS

EDITOR'S DESK

PHOTOGRAPHY BY DAVID BOWMAN

The Triple Option

What do you think about in April? Filing taxes? Driving with the windows down? I've got the NFL Draft on my mind. After 330 football players tried to dazzle coaches at this year's scouting combine, I'm curious to see how each franchise's team-building strategy unfolds. Some coaches seek an indomitable defense. Other coaches want a third option in their passing game. And teams that desire someone new for every position have plenty of options.

IBM clients also have multiple options with their cloud deployment strategies. This month's cover story highlights a whitepaper authored by analyst Julie Craig at Enterprise Management Associates, which dissects all the ways that IBM Power Systems* clients can achieve the cloud model their organization wants. Do you want to construct and run a public cloud? Do you want to connect a private cloud to a public cloud? The article on page 18 explains what's available to implement your strategies.

Elsewhere in the issue, we cover the cloud-based disaster recovery (DR) journey of Chilewich Sultan, a textile creator and manufacturer. After Hurricane Sandy left the company's computing environment down for five days, the company decided to move to another platform and upgrade to a more robust DR solution. Read more on page 14. We also examine how chargeback systems are a growing concern. To learn about five main flaws in current chargeback systems and what IT organizations should do to address those issues, turn to page 10.

The Tech Showcase on page 25 analyzes the importance of upgrading system security strategies. Terry Ford, team lead for Security Services Delivery, IBM, helped build a security assessment tool that administrators can use to find system areas which are vulnerable to a hacker's attack.

While one team's Plan A can be upended by another team's selection in the NFL Draft, IT teams don't have to worry about that. Plenty of options exist to help enterprises implement a customized public, private or hybrid cloud solution that can push business over the goal line. P

Jessica Tam // Managing Editor
jtam@msptechmedia.com

CONTRIBUTORS

Gene Rebeck

Duluth, Drafts and a Dog

Gene Rebeck is a freelance writer specializing in business, technology and economic development. He wrote the Tech Showcase on page 25. Gene lives in Duluth, Minnesota, where he enjoys savoring locally crafted beers, strolling with his dog among the area's many bucolic landscapes, and exploring the old industrial and railroad sites that are also abundant in his neck of the North Woods.

Andy Potts

Illustrations in Living Color

This month's cover art is the handiwork of Andy Potts. He grew up drawing and painting, realizing early on that he wanted to "make pictures" when he got older. In his youth, Andy was hugely influenced by the work of Syd Mead (visual designer in the films Bladerunner, Aliens and Tron) along with sci-fi/fantasy artists H. R. Giger and Chris Foss. After taking a foundation in art course in 1991 at Stourbridge College, he discovered that illustration could become his career. Today the illustrator and motion designer is based in London, creating commissioned pieces with a style that's a digital blend of collaged textures, photography and hand-crafted elements.

Buying Time for Cybersecurity

Tool enables IBM i administrators to assess security weaknesses

By Gene Rebeck

Even with more public awareness about security breaches in recent years, it's surprising that "security administration isn't given the priority it should," says Terry Ford, team lead for security services delivery, IBM Systems Lab Services in Rochester, Minn. "Administrators don't regularly look at it, or they only look at it after performing other work."

Still, Ford believes that they're not intentionally negligent. Administrators are often frustrated because they'd like to do more security checks, but budgetary constraints stop them, he explains. "Yet they will be the ones who are held accountable if they aren't able to practice secure computing with the rigor it requires."

Why don't organizations examine security as closely as they should? "Time is a big part of that," Ford says. Companies focus on producing and selling products or services, so security is often an afterthought, he notes.

To help IBM i clients, Ford and his team built a security compliance, assessment and reporting tool (CART) that allows time-starved administrators to examine where hackers could exploit their systems. (Other IBM teams have created similar assessment tools for AIX* and Linux* administrators.) The CART provides a comprehensive picture of a client's systems and pinpoints current and potential weaknesses. The tool creates daily reports but also features an alert function when changes occur for system administrators who can't review every report.

Saving IBM i administrators valuable time, **CART** reports on more than 1,000 data points related to security, configuration and statistics

The Bigger Picture

The lack of time focused on security is just one problem. In Ford's opinion, many organizations are "often ignorant, or choose to be ignorant, about the dangers of a security breach." They think a breach won't hit them

> "What the smaller guy fails to realize is that a hacker's path to the larger organization may be through him, a smaller but related company or supplier."
>
> —Terry Ford, team lead for security services delivery, IBM Systems Lab Services

because their business is too small. With news about major retailers, internet service providers and financial services firms that suffered expensive data breaches, they believe that hackers prefer to target larger organizations. There's some truth to that, Ford notes. "But what the smaller guy fails to realize is that a hacker's path to the larger organization may be through him, a smaller but related company or supplier," he adds.

Organizations try to keep their systems secure by having at least a firewall or password access system. But Ford notes, "Hackers are more educated than system administrators are." He explains that hackers have made it their job to outwit the latest cybersecurity fixes and strategies. And few companies can devote the same kind of full-time resources to system security.

Several vendors offer IBM i security solutions. They have very good monitoring and remedial products, Ford says. "However, they tend to be high-level and do not go deep enough," he adds. "Because of this, clients are sometimes given a false sense of security when they may have unknown configuration items such as with DDM or SSH, leaving their system at risk."

Monitoring tools can help. But if an assessment hasn't identified a weak point, "it means the weakness is still present," Ford notes. "A comprehensive assessment solution with monitoring can help clients determine the extent of their weaknesses and provide information for a proper root cause analysis in remediating the weakness."

Not-So Secret Passwords

Another problem security administrators face is when user profiles and passwords are weak points. Even though they're designed to block hackers, Ford believes too many users have passwords that can hand cyber thieves the key to their employer's data. "The easiest hack for many cyber pirates is using default passwords or dictionary passwords," he notes. The default password is the easiest as it's usually the same as the user name. Dictionary passwords include movie titles, names of sports teams, family names and other popular cultural references. Users also often use the same passwords for all the systems they access. Once access is gained to one system, all connected systems are at risk.

SPONSORED ADVERTISING CONTENT

Mandatory Security Reporting Intensifies for All Merchants

One million: a huge number. When asked how many credit card transactions are processed each year, most answer: "Less than 1 million." Until Jan. 31, that excused you from mandatory security audit reporting to your bank.

However, now even the lowest volume merchants must submit a PCI Self-Assessment Questionnaire (SAQ), and an Attestation of Compliance (AOC) signed by an officer of your company stating its accuracy. If you touch card data with your workstations—ever—that SAQ will be the draconian SAQ "D"—19,000-plus words asking over 500 intrusive, technical and operational questions, possibly requiring months to research.

The payment industry is moving toward more ponderous reporting from you. Be alert and diligent. The bank notices are on their way. This will intensify.

After 24 years in this niche, we see an unprecedented level of anxiety and activity at the card brands. The rules for securely handling credit cards are changing rapidly, and the simplicity of the past is being challenged. Integration with remote tokenization is part of the answer.

Ira Chandler
CTO, Curbstone Corporation

Author of the first commercial AS/400 credit card software in 1993, Ira and Curbstone focus on IBM i payment security.

> "Using 10,000 well-known passwords discovered in reported breaches, we can calculate and compare whether a user or administrator's password is on that list." —Terry Ford

The IBM i CART hunts down these easy passwords and their variations. "We have created a tool that actually does a dictionary check of its users' passwords," Ford says. "Using 10,000 well-known passwords discovered in reported breaches, we can calculate and compare whether a user or administrator's password is on that list." With that knowledge, security administrators can encourage users to create more complex passwords—or disable their account until a more complex password is entered.

Identifying unsecure user names and passwords is a small part of the CART's function. "We report on more than 1,000 data points related to security settings, configuration and statistics of system use," Ford says. "With this, a client can observe changes over time or perform various types of trend analysis related to security. There are probably millions of other pieces of information that we're scanning through and interrogating to see how it's accessed and who owns it. We don't look at the content of any file. We simply check to make sure a backdoor isn't present in any of those objects."

An event-monitoring component is also included with the CART. This gives clients a more granular look at security events across all of their enterprise's IBM i systems in real

Learn More

Visit the IBM developerWorks page on IBM i Security Services, Monitoring and Reporting, at:

ibm.co/2lAR6fZ

SPONSORED ADVERTISING CONTENT

Key Considerations for IBM i SIEM Integration

The IBM i is increasingly becoming an integral part of the "big picture" for enterprise security and integration with security information event management (SIEM) solutions.

With the expectation that many large enterprises as well as small to medium companies will integrate IBM i data with a SIEM, consider the following three points when thinking about the integration:

1. It's more than just QAUDJRN. Additional types of security information that can be sent from the IBM i include information related to exit point activity, anti-virus results, QSYSOPR messages, authority changes, field-level database changes in applications and more.
2. Be granular. Establish the right data points and configure the right data to go to the enterprise SIEM solution. A "send everything" strategy takes up more resources, is less effective and often doesn't help a security team uncover threats.
3. Focus. Enterprise security teams want to correlate data across the enterprise, but aren't necessarily looking to step into the IBM i world. Providing the right data to an enterprise SIEM and security team is only one step in the process. In addition to sending data to SIEM, focus on alerts local to the IBM i to keep multiple checks in place.

Jatin Thakker
COO, Software Engineering of America

As COO at SEA for 11 years, Jatin has helped hundreds of customers achieve enterprise-scale security, auditing and monitoring on the IBM i platform.

time. "It can then alert those who need to know of their occurrence or report on them from the central data mart," Ford says. "We also provide a utility for customers to add or create items or events of their interest."

The Gift of Time

Over the past four years, the CART has become a flagship item in Lab Services' portfolio, and it's based on IBM's security assessment tool, which has had more than two decades of development. But it's always evolving. Lab Services continually aims to provide better systems and security management because Ford notes cybercriminals are constant threats.

"We try to automate as much of our assessment process as possible—what we can reliably and comprehensively do in the shortest amount of time," he adds. "We have derivatives of our tool that create an even more comprehensive view of security. That's work we continue to enhance and develop."

Ford's team at Lab Services constantly seeks ways to update the CART tool to provide value to the IBM i community. If system administrators can only devote one day a week to security, Lab Services can still provide them with "a picture of what changed in their environment so that when they do get the time to look at security, they can hone in on the things that have changed," Ford says. "Or, with our event monitor, the client can respond immediately to events."

In the future, "We'll add more metrics, more configuration items and security analytics," he says. "When we designed and developed the tooling, it was a collaboration with many subject matter experts—first and foremost, the DB2* for i consultants here in Lab Services. This team helps clients get more value out of data through analytics. And that was at the heart of what we wanted to provide relative to security."

Save Time, Save Money

Ford describes the CART as a kind of time machine, as it captures what has been going on in a client's systems and makes predictions on how it could look in the future based on the current operating mode.

Most clients who need to assess and monitor their systems are very time-conscious, according to Ford. Unfortunately, they can't afford to spend the time to analyze everything on the system. Yet they need to be aware of what's going on within their systems. With CART, he notes, "we have created a tool that helps them buy the time they need to find what is going on." P

Gene Rebeck is a freelance writer based in Duluth, Minnesota.