TAG-ITI

Talal Abu-Ghazaleh Information Technology International

Newsletter

SEPTEMBER 2017 | ISSUE 16

IN THIS ISSUE

Talal Abu-Ghazaleh Organization and Ministry of Interior Discuss Means of Cooperation

AMMAN- HE Dr. Talal Abu-Ghazaleh received Governor Mohammad Al-Kharisha, Director of Administrative Affairs, Human Resources and Performance Development and Governor Mohammad Al-Sarhan, Director of Local Development at the Ministry of interior, to discuss means of cooperation in the field of services provided by Talal Abu-Ghazaleh Organization (TAG-Org).

Dr. Abu-Ghazaleh highly commended the continuous efforts offered by the Ministry, in serving all members of the society emphasizing the Ministry's role in the life of citizens.

The two parties discussed the provision of training programs through Talal Abu-Ghazaleh Academy in accordance with the Ministry's training needs.

They agreed to sign a Memorandum of Understanding that includes cooperation in applying the E-government system, teaching English as TAG-Org is accredited from Cambridge English Language Assessment, and providing digital academic qualification programs for the Ministry employees.

Meanwhile, TAG-Org and TAG-Knowledge Society has concluded the first training course for the Ministry employees entitled, "Secretariat's Codes of Practice and Procedures."

The three-day course for secretaries of governorate councils, focused on their tasks and their role in applying the new Decentralization Law.

The training course is part of TAG-Org's initiatives to serve governmental institutions by developing their employees' skills, building their capacities, and supporting different institutions based on the Organization's role in fulfilling its Corporate Social Responsibility.

Dr. Omar Al-Trawneh, a specialized adviser in Human Resources Development, briefed the participants on secretary tasks, how to prepare reports, how to take notes and minutes of meetings, the distinction between the basic legal concepts and the legislative and regulatory requirements, and other subjects. There was also focus on the importance of their role in supporting the Councils' decisions and its effectiveness, which contributed to the development of the municipal councils.

Cooperation between TAG-Org and the Ministry of Interior is an application of the visions of HM King Abdullah II in enhancing partnership between the public and private sectors in various fields.

Certificates were presented at a graduation ceremony to the 27 participating secretaries from the governorate councils.

Global Cyberattack on Energy Sector Stokes Deep Fears

The hacker group known as "Dragonfly" is behind sophisticated wave of recent cyberattacks on the energy sectors of Europe and North America, Symantec reported Wednesday.

The attacks could provide the group with the means to severely disrupt energy operations on both continents.

Dragonfly launched a simililar campaign from 2011 to 2014, but it entered a quiet period in 2014 after Symantec and others exposed its activities.

The current campaign began in December 2015, Symantec noted.

The firm found strong indications of Dragonfly activity in the United States, Turkey and Switzerland, and traces of activity in places outside those areas.

The attackers have employed a number of methods to infect systems, including malicious emails, watering hole attacks and Trojanized software.

Gravity of Situation

"Breaching of multiple energy sector organizations is extremely concerning," said Eric Chien, technical director of Symantec's Security Response and Technology Division.

"The U.S. power grid is large and complex, and there isn't a single switch that turns off the electricity for the entire United States," he told TechNewsWorld. "However, access to operational systems within multiple energy sector organizations could lead to significant disruption."

Although the impact of the attacks so far has been minimal, that doesn't mitigate the need for concern.

"The future is what's at play here," said Dana Tamir, vice president of market strategy at Indegy.

"This might be an attempt to gain information about these systems in preparation of future attacks," she told TechNewsWorld. "The fact that nothing's happened right now doesn't mean that nothing will happen in the near future."

Unclear Motives

Security researchers have yet to determine the motives behind the energy sector attacks.

"We are not seeing any motivation in regards to monetary, extortion or economic espionage," Symantec's Chien said.

"We do not know the ultimate motivation of the attacker, but clearly disruption and sabotage are candidates with access to such systems," he added.

The characteristics of the attacks point to a class of perpetrator, observed Indegy's Tamir.

"The sophistication of the attack, the targets of the attack, the gathering of information indicates there's a bigger play here that's more typical of a nation-state than a criminal organization," she said.

Tools of the Trade

While the campaign itself is sophisticated, the tools and methods used by the attackers to penetrate the SCADA industrial control systems are not.

"What's interesting here is the relatively unsophisticated methods the hacking group has used," said Leigh-Anne Galloway, cybersecurity resilience lead for Positive Technologies.

"Usually with SCADA, the tactic of choice is to exploit zero-day vulnerabilities," she told TechNewsWorld. "In this case, though, they've chosen to go for the older but most-effective methods of phishing and watering holes to get in."

The Dragonfly hackers use their tools to collect credentials and perform reconnaissance on the systems they're attacking, noted Indegy's Tamir.

"Once they get that information and penetrate the systems themselves, manipulating the systems does not require any special tools," she said. "The systems are quite easy to manipulate once you're inside them."

"We are seeing the attackers increasingly 'live off the land' by using default system administration tools in order to penetrate systems, as well as reusing and modifying existing off-the-shelf malicious software," added Symantec's Chien.

Countering the Attacks

Since discovering the latest activity, Symantec has briefed more than 100 energy sector and government organizations in the United States and Europe and made recommendations to them about coping with the attacks.

"The power grid penetration incidents are terrifying," said Varun Badhwar, CEO of RedLock.

"They really hit home the importance of having a solid cybersecurity strategy in place for organizations of all types," he told TechNewsWorld.

Attacks on industrial control systems have been increasing in recent times, according to a new report from IBM Security.

There were 2,788 attacks in 2016, up from 640 attacks in 2013, for instance. That trend appears to be continuing this year. Through July, IBM already had reported 2,522 attacks.

"There's growing awareness," Indegy's Tamir observed, "but the energy sector is moving too slow to address these threats."

Source:
http://www.technewsworld.com/story/Global-Cyberattack-on-Energy-Sector-Stokes-Deep-Fears-84790.html

Microsoft Releases Long-Awaited Security Tool

Microsoft has released its long-awaited cloud-based bug detection tool, previously code-named "Project Springfield." The Windows version became generally available, and a new Linux version became available as a preview last week.

The tool, Microsoft Security Risk Detection, uses artificial intelligence to hunt down security vulnerabilities in software that is about to be released.

Microsoft Security Risk Detection will help developers do fuzz testing, said David Molnar, the Microsoft researcher in charge of the group that developed the tool. Fuzz testing normally is done using outside consultants to test new software. Its purpose is to make sure vulnerabilities can be weeded out before the product goes into wide release to avoid the necessity of patching them on the back end.

The service uses artificial intelligence to ask particular "what if" questions about new software, focusing on critical areas that might be vulnerable to attack by bad actors.

Microsoft first released a test version of the service last year. Docusign, a firm that specializes in automated electronic signatures, is one of the companies that volunteered to try it out.

The tool helped Docusign weed out bugs in its software and almost never returned false positives, according to John Heasman, senior director of software security at the company.

The low rate of false positives is very important, he said, because companies typically have to spend a lot of time tracking down false positives, which uses time that otherwise could be devoted to investigating legitimate threats.

In-House Technology

Microsoft has been using Sage, a key component of the service, since the mid-2000s to test versions of Windows, Office and other products. Several product teams at the company use the service as part of the Microsoft Security Development Lifecycle.

Microsoft plans to offer the tool for sale later this summer through Microsoft Services.

Prevent Defense

The release is meaningful, according to Dustin Childs, communications director for the zero day initiative at Trend Micro, who noted that the service gives developers access to security testing they otherwise might not use.

"Bugs are much easier to detect during software development," he told LinuxInsider, "so enhanced testing prior to release could prevent security problems down the road."

Whether companies embrace the service depends largely on how many false positives they get, Childs said. Another important issue will be the trust issue between developers and Microsoft, which could depend on how much information is shared with the developers and how much is retained by Microsoft.

From Microsoft's perspective, the gain is twofold, said Childs. The service will help Microsoft create a safer ecosystem running a series of Windows applications, and allow the company to show off its cloud computing and AI capabilities. The service also will introduce Azure to a large community of potential customers.

Security is something that everyone wants, but few are willing to shell out the money for it, observed Jim McGregor, principal analyst at Tirias Research.

"IT managers often stick with the security solutions they are familiar with and upgrade with budgetary cycles," he told LinuxInsider.

The industry rarely works together to resolve security issues, McGregor said.

True IT security requires hardware and software to be effective, he pointed out.

However, Microsoft's solution takes security to a new level by combining AI and cloud resources, said McGregor. It continuously leverages a wide range of information and reacts to new threats faster than traditional solutions.

"It's not clear how much success Microsoft will have with this new service," he said, "but every IT manager should be looking to AI for improved security."

Source:
http://www.technewsworld.com/story/software/84697.html

Robots May Become Go-To Customer Service Reps

The customer service robot market will be worth US$88 million by 2022, according to a report Tractica released earlier this week. Annual shipments are expected to increase from 2,730 units in 2016 to nearly 4,800 in 2022.

The robots will be both humanoid and non-humanoid. However, telepresence robots, chatbots, and stationary customer interactive systems that don't have moving parts are not included in the count.

Nearly half of all customer service robots will be deployed in the Asia Pacific Region; other significant markets will be North America and Europe.

Demand for customer service robots is driven by the following factors, according to the report:

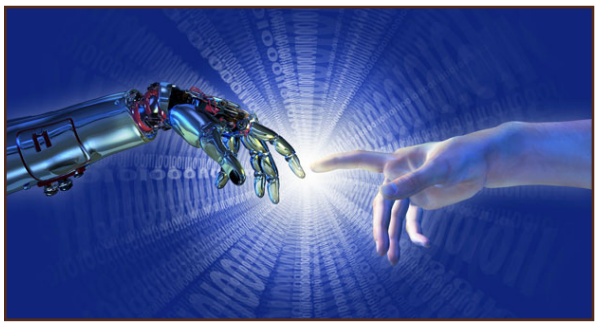
- interactive marketing and re-branding strategies;
- the cost of human staff;
- customer service digitization and competition;
- robotics as a tool for customer behavioral analytics;
- the shifting roles of human staff; and
- initiatives to promote robots for the service industry, particularly in Japan and China.

Jobs for Robots

Robots will be useful in situations where customer interactions are standardized and repetitive -- such as in banks, shopping malls, family entertainment centers, exhibitions and events, airports and stores, Tractica noted.

Robots "can pick up where self-service in kiosks leaves off by humanizing some of the capabilities and using other sensory areas such as vision, hearing and speech to improve engagement," said Ray Wang, principal analyst at Constellation Research.

"The demand's coming from the automation of lower-skilled white collar jobs," he told CRM Buyer.



Japan's Henn-na Hotel, for example, is fully staffed by robots, Wang pointed out.

A number of organizations already are using robots on a trial basis in the United States:

- Mineta San Jose International Airport began using three customer service robots in 2016;
- Lowe's introduced an autonomous retail service robot in 11 of its stores throughout San Francisco in 2016, and retail service robots also are being deployed in its OSH stores;
- Target ran a one-week test at one of its San Francisco stores, using robots to help stock shelves and take inventory; it is considering building a concept store staffed by customer service robots.

China's EVA Air and Japan Airlines are using customer service robots, as are Alaska's St. Mary's Airport, Scotland's Glasgow Airport and Japan's Haneda Airport.

With instant access to a corporate database, robots will reduce dramatically the amount of time wasted when dealing with customer queries.

Robots "are wrong less often," observed Rob Enderle, principal analyst at the Enderle Group.

Also, "they never have a bad day, they can more easily multitask, and they're a novelty people might go to a store to see," he told CRM Buyer.

"People spend or waste a huge amount of time looking up information that should be instantly at their finger tips," said Alan Lepofsky, principal analyst at Constellation Research.

"Content is not king -- context is," he told CRM Buyer.

The Downside of Robot Deployments

In addition to market challenges, the customer service robot industry faces technological issues related to human-robot interaction, navigation autonomy, machine vision and speech recognition, AI and machine learning, the limitations of cloud robotics, and safety and standards, Tractica noted.

Robots can deal with simple questions, said Cindy Zhou, principal analyst at Constellation Research.

However, "customers still look for humans for any real assistance with problems," she told CRM Buyer.

Consumers mainly regarded the robots they encountered at banks, restaurants and stores in Tokyo as a novelty to play and interact with while waiting for human service, CNBC recently reported.

"People aren't used to trusting robots yet," Enderle said. "The robots at San Jose Airport, for instance, seem to stand alone most of the time."

That could change over time -- or robots could fade from the scene.

The disruption caused by Amazon could squash the demand for robots in customer service, Enderle suggested.

"For instance, in 2022, Lowe's may have to shift to more of an Amazon delivery model than a store model," he said, "making the need for these robots near nonexistent."

Source:
http://www.crmbuyer.com/story/84765.html

For More Information:

Talal Abu-Ghazaleh Information Technology International TAG-ITI

Shahid Halling – TAG-ITI

Tel: (0962-6) 5100900
Fax: (0962-6) 5100901

Or you may reach us electronically through our website:
TAGITI.com

And our email:
shalling@tagiti.com

This newsletter is published by:
Talal Abu-Ghazaleh Information Technology International (*TAG-ITI*)