Volume XXII 2019
ISSUE no.1
MBNA Publishing House Constanta 2019

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Using cognitive computing for a secure cloud in the energy sector

To cite this article: S. Eftimie, R. Moinescu and C Răcuciu, Scientific Bulletin of Naval Academy, Vol. XXII 2019, pg. 52-58.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-19-I1-007

Using cognitive computing for a secure cloud in the energy sector

S Eftimie[1], R Moinescu[2] and C Răcuciu[3]

[1] Ph.D. Student, Military Technical Academy
[2] Ph.D. Student, Military Technical Academy
[3] Prof. Eng. Ph.D., Military Technical Academy

Abstract. The evolving changes in the energy industry have led to increased efforts in adopting cloud technologies. In this paper, we explore specific security needs of the energy sector and propose a solution that uses the latest advances in cognitive computing to detect malicious insiders, one of the top threats that prevent cloud adoption.

1. The energy industry transformation

The energy sector is currently in a process of fundamental transformation at a global level. It is expected that in the next five to fifteen years a major disruption will take place in the industry [1] that will affect key players. This revolution is powered by extensive efforts on reducing carbon emissions, climate impact reduction and a turn to a more efficient energy ecosystem that harnesses the latest technologies. The actual linear distribution chains will be replaced by dynamic energy systems that will be more sustainable and which will support two-way energy flows as opposed to the conventional one-way distribution. This will encourage clean energy and the competition between the different actors will lead to innovation.

The major challenges faced by businesses that are operating in the energy sector are the operational and maintenance costs with the goal of maximizing the asset use and productivity and the responsiveness to the changing standards and customer demands. The cloud and its business model are a solution for specific challenges faced by energy companies such as an efficient administration. Companies can manage their critical documents on private clouds. This reduces the friction for customer-centric activities, which in return stimulates marketing and increases sales. In addition, document sharing and management lead to streamlined change management.

Another advantage of the cloud is the ability to deliver analytical insights to the business operations which can be used to develop measures for optimizing the resource usage. In addition, operational cost reduction can be achieved by using a distributed approach that leads to savings in energy consumption, while declining the proportion of equipment failures. The final cost is also reduced for the end user due to the pay-as-you-go model.

Security has been identified as the main concern of adopting cloud services. Although direct intrusion resulting in blackouts is the most obvious threat in the energy industry, other threats related to the user data are also a major source of impending problems. Security issues can have broader implications such as effects in a state's economy. In the next section, we will explore the types of malicious insiders in the context of the energy sector. Insiders have become a growing threat in the past few years and conventional security solutions struggle to keep up with the new challenge.

2. Insider threats in the energy sector

Energy businesses, as part of the state's critical infrastructure, are a target for threats from malicious outsiders aiming to do damage and disrupt essential operations. While powerful physical and cybersecurity measures usually are in place to prevent and detect these types of incidents, similar measures have not been created to address threats from insiders. Insiders, including workers, delegated workers, guests and trusted third parties, often have unrestricted access to classified and critical information, systems, and resources for which there is negligible supervision or monitoring. Insider threats have emerged in the past few years as one of the main security issues in cloud computing. According to a recent study [2], over 90% of organizations consider themselves vulnerable to malicious insider attacks. On one side the cloud adoption and the BYOD (bring your own device) policies have streamlined businesses activities but have also eased the access to confidential data. According to the same study, 53% confirmed that they had experienced an insider attack in the last twelve months.

Insider breaches namely breaches produced by employees and even leaders within a company are among the hardest to detect of all data breaches. The cost of these breaches is also among the highest. According to a study done by IBM [3] more than 70% of total compromised data was caused by unintentional insiders. The study concludes that insider threats are the cause of 60% of all cyber-attacks.

Considering that the organizations usually focus substantial resources on handling external threats, insiders are expected to cause an even larger economic threat to the organization. A 2018 study [4] shows that the average cost of incidents caused by insiders was greater than $8 million in 2017.

Insider threats have traditionally been approached with training that raises awareness in order to reduce risks. As we will see in the part where we describe the different types of insiders, these activities are important, but they're not sufficient to mitigate all types of risk. Humans are extremely inconstant and failing to address all types of insiders might result in expensive security incidents.

The 5 types of insider threats according to IBM [3] are Non-responders, Inadvertent Insiders, Insider Collusion, Persistent Malicious Insiders and Disgruntled Employees.

The *Non-responders* represent a small but still considerable fraction of the worker population that are not responsive to the different awareness exercises. This type of employee is among the riskiest because it has been found [4] that individuals with a strong record of failing to recognize phishing campaigns are most likely to be phished again. It's important to know that these users may not intend to act negligently but they do pose a risk as we can see in a 2017 [4] study that shows that more than 4% of people targeted in any given phishing campaign will engage in the activity. According to a research study [4], 63% of security incidents recorded in 2017 were caused by all categories of negligence among the employees.

Although workers who regularly act in vulnerable circumstances are usually a small fraction of the population, the total effect of employee errors is astonishing. Regarding the cost associated with these events, a study [4] showed that more than 60% of the incidents in 2017 were caused by different categories of negligence.

The Inadvertent Insiders category is characterized by simple negligence and is the most expensive employee risk category as previously mentioned. Inadvertent insiders cause breaches due to isolated mistakes although they generally display a secure behavior and comply with company policy.

Threat agents are increasingly becoming aware of the vulnerabilities caused by inadvertent insiders. An analysis of the common criminal methods used to exploit employee error revealed some patterns: 38% of external actors attempted to deceive users into accessing a malicious attachment or link, 35% of the external attacks were man-in-the-middle attempts and 27% of external threats attempted to exploit servers that were misconfigured.

Insider Collusion represents a threat which is defined as insider cooperation with malicious external actors. This is a rare form of criminal insider risk, but it's nonetheless a considerable threat since cybercriminals are known to recruit agents. Collusion incidents usually take the form of fraud [5], intellectual property theft or a combination of the two. Insider-caused events, which include collusion, are among the priciest types of a breach and may take four times longer to identify than events caused by insiders who operate by themselves.

Persistent Malicious Insiders represents a category of criminal insiders that steal data with the goal of financial gains. A study [6] on criminal insider threats found that 62% of insiders with malicious intent are people pursuing an additional source of revenue. This type of criminal can remain undetected by using sophisticated data exfiltration techniques. The slow exfiltration of data is often utilized instead of completing significant data exports which could trigger alerts in conventional network surveillance tools.

Disgruntled Employees are employees who execute premeditated sabotage or intellectual property theft. Disgruntled employees can pose some of the costliest risks to a business. A study [6] showed that 29% of the criminal insiders stole information after resigning or being fired for the purpose of future gains. Only 9% were motivated by simple sabotage.

Disgruntled personnel can fit many behavioral sub-patterns. Some angry workers may start searching for sensitive information without having a specific goal in mind. Other workers may have very particular intentions at the moment of their resignation and may plan to sell trade secrets to competitors.

Although human endpoints are among the biggest vulnerabilities in an organization, insider threats are variable. There is no single methodology which can alleviate all categories of insider risk. Improving the knowledge and awareness of the employees is probably the best way to protect against insider threats. All things considered, even awareness training will not alleviate the risk of non-responders. Other solutions need to be considered for this category of insiders such as tools for behavioral analytics. When addressing the insider problem, data protection is the place to start. Valuable data is vulnerable irrespective of the type of insider threat. In order to create transparency, companies should determine and categorize data assets that are vulnerable and protect them both against negligence and criminal intent.

Behavioral analytics can be used to detect variations in an individual's behavior pattern and despite the unicity of the behavior, this can be a powerful tool for detecting risks in subtle patterns of workplace practices and information utilization. Deep analytics using user behavior characteristics has the potential to reduce all categories of insider threat risk.

Risk scoring represents the next step. Applications for behavioral analytics have the ability to allocate risk scores to identify potential insider risks in a proactive manner. When staff members are at increased risk for mistakes or criminal conduct is recognized, companies can react with mitigating mechanisms, reinforced access management or even account quarantine to prevent data loss.

Addressing elementary vulnerabilities in enterprise security represents one of the greatest defenses against both insider and external threats. Compliance measures, when are properly maintained, can facilitate data transparency and protection for critical assets. Network monitoring can expose compromised systems or insider threats in a timely manner.

Statistically speaking, insiders are the cause of most data breaches. Negligence, malicious insiders and stolen credentials were linked to the majority of lost records last year. According to IBM [3], there is a 5% per year increase in the occurrence of insider threats.

The key to adequately address the insider problem is using the latest technologies in detecting malicious behavior. While behavioral analytics exist for some time, new advances have been made in cognitive computing. Cognitive computing systems are a blend of computer science and cognitive science. Cognitive computing algorithms use data mining and natural language processing in ways that are better than conventional security solutions.

Recognizing the subtle variation in human behavior is important in creating acceptable safeguards against insider risks. By using user behavioral analytics tools, strong compliance measures, and data protection mechanisms, it's possible to proactively detect and respond to patterns of risk in human behavior.

In the next section, we will analyze how cognitive computing can help in the early detection of the different types of insiders and alleviate the risks involved with humans.

3. Detecting insiders

Several studies have shown that human language reflects the personality and emotional states [7] of an individual. This theory is put to practice in advertising, marketing, and other related fields. Cognitive computing is currently used for detecting and categorizing types of personality in order to better implement targeted marketing schemas and to create new products that better suit their customers. The end goal is to match the proper offerings to the most responsive customers, increasing both the efficiency of the offers and the customer fulfilment.

Cognitive computing services such as IBM Personality Insights have successfully been configured to use social media data in order to develop richer portraits of customers through analytics. The results have been used to segment customers and create marketing schemas that are both more relevant and more intimate.

Some of the results of using this novel technology are:

- Detection of indicators of intentions in near real-time.
- Creation of individual portraits that include fundamental psychological inclinations, which can influence choices performed by individuals
- Creation of highly personalized strategies that are based on intrinsic and behavioural preferences
- Engagement of the appropriate target audience at the best time to introduce efficient marketing campaigns.
- Manage brand loyalty by providing individualized products and services that customers desire
- Identify, based on social data high-value clients from among millions of members
- Identify business opportunities to test new offerings by making new products available to individuals who are more likely to use them.

What we propose is to use the same technology to identify malicious insiders based on personality profiles. The use of artificial intelligence has become a hype in the present days. It is more likely to find keywords such as AI attached to all kind of products in order to drive sales. Despite this, few AI-driven security solutions exist on the market. The majority of solutions on the market are closed source and the amount of research papers in this field is scarce. Despite several cases in other industries where cognitive computing has successfully interpreted and filtered colossal amounts of data that were impossible to be absorbed and applied by humans only, cybersecurity has not yet reached a point where it fully takes advantage of the technology. Cybersecurity has been traditionally a continuous process of integrating access controls at recognized exposed locations based on procedures and policies. Controls are then examined in order to identify areas requiring extra rules and policy improvements. These represent essential security practices that are employed efficiently across organizations, using comparable tools, procedures, and expertise. Faced with an evolving threat landscape, many organizations find that their traditional security frameworks are not keeping up with the latest challenges.

Cognitive computing applied in security is different from the basic behavioural anomaly detection. AI may not even be necessary to detect anomalies because patterns and procedures can uncover such alerts. Cognitive computing is about interpreting events based on continuous learning that enhances a corpus of knowledge. While it has the ability to identify behavioural discrepancies, a cognitive solution can perform its own evaluation and develop its own assumption. Going back to the malicious insider problem, we will start by addressing the types of insider threat mentioned in the previous section of this paper and propose a technical solution that involves cognitive computing. Personality Insights from the IBM Watson service suite is currently the only accessible service that implements cognitive computing. This service is built on the psychology of language combined with data analytics algorithms. The service analyses a specific content and returns a personality profile for the author of the content. The service has the ability to identify personality characteristics based on three dimensions: a model that generally describes how an individual engages with the world, needs, and values of the analysed individual.

We will proceed by describing the framework that we propose for detecting insiders. In Fig. 1 we can observe the structural components of the framework having cognitive computing as a central part of the process. In order to address the different type of personalities associated with the different types of insiders, we added an additional component that is represented by a so-called honeypot. We addressed the topic of honeypots in a past work [8]. In this case the honeypot is a production one and works by improving the security posture by detecting attacks and gives less information about the modus operandi of the attackers. Its usefulness will become apparent when we go into different types of insiders. Monitoring the employee conversations is a common practice inside organizations. When we consider insiders, we acknowledge that this type of threat can exist both at the cloud provider and at the premises of the energy company [9]. Both scenarios should be taken into consideration. The framework uses a service that is placed in the cloud and that can process the communications that an individual produces in the form of corporate chat and emails.

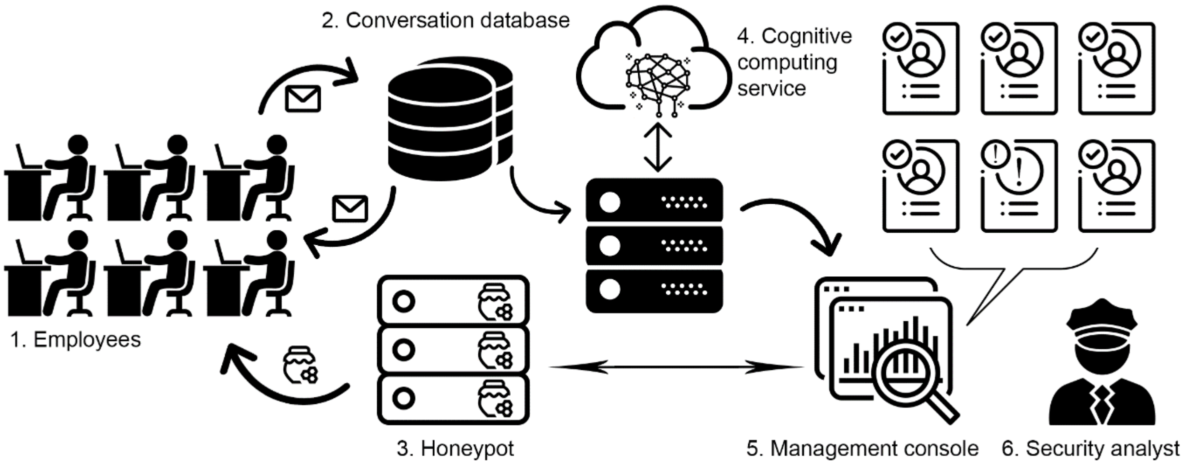

Fig. 1. Cognitive computing framework for insider detection

The flow of the framework begins with the conversational database (2) generated by the employees (1) of an organization. In addition, a strategy should be developed by the security office in order to model and prioritise the type of assets that can be targeted or affected by insiders. The conversations are analysed by the cognitive computing service (4) and results are displayed in the analyst's (6) management console (5). The security analyst is also in charge of deploying honeypots (3) that are developed according to the insider management strategy.

The role of the analyst becomes more creative and resembles more with the one of a criminal profiler or investigator. The analyst must find creative ways to deploy honeypots.

The non-responder insider threat needs a special approach since the targeted staff is unaware and is likely to remain unaware of possible attacks. A strategy to diminish this threat would be to first identify the staff members that fit this group. This can be achieved by deploying a honeypot that involves fake phishing attempts correlated with personality traits of the victim. Once the group is identified and flagged accordingly, special measures should be put in place to limit the potential damage inflicted by this group. This can include restrictions and special approval schemas. Cognitive computing can be used in tandem with the honeypot solution in order to improve the knowledge core and to better detect this type of personality. Another potential use of cognitive computing that is not present in the current framework would be to analyse the content of the emails in order to detect phishing, thus the non-responders would be protected. Unfortunately, this type of insider threat cannot be fully addressed in the context of technology. Incompetent staff should be relieved of the duties if it demonstrated that it cannot handle common-sense security practices.

Addressing the inadvertent insiders using cognitive computing can be realised by identifying the personality type of the target individual and propose approaches that take the personality in consideration in order to maximize the effectiveness of the training by selecting targeted individuals. These individuals are not malicious by default and they should be educated in order to not make costly mistakes related to security. Cognitive computing can help by identifying the appropriate strategy in order to maximize the effectiveness of the training in the same way highly personalized strategies are made based on intrinsic and behavioural preferences. In this way, the engagement of the appropriate target audience is optimized in order to maximize the efficiency of the training.

Insider collusion can be addressed by cognitive computing by analysing the conversation between different staff members. The algorithm that is used to detect brand loyalty can be set to detect in a similar manner adversity towards the company or the management or a different member of the staff. Changes in the emotion regarding these factors should be kept in time in order to correlate them with events such as year ends when employees can get disgruntled.

Persistent malicious insiders are hard to identify due to the fact they are most likely experts in their field and know how to remain undetected. Sentiment analyses and profile matching to a target criminal profile can be used to detect malicious intent. Flagging them and using behavioural analytics can be deployed on top of the sentiment detection in order to check for malicious actions such as data exfiltration.

Disgruntled employees can be detected by constructing an emotional profile based on their conversations and detect adversity towards the company, company values and management.

The cognitive part is composed of a series of complex knowledge structures that humans are not able to fully understand in terms of function. It seems that the next decades in terms of computing will be marked by an increasing prevalence of machine intelligence for which the inner workings cannot be comprehended by the human mind.

4. Conclusions

The energy sector is going through a fundamental transformation in the quest for efficiency. The many advantages of cloud such as business scalability, market flexibility and cost elasticity, that are also beneficial for other industries are also finding their way into to the energy sector. By utilizing scalable computing resources, energy companies can achieve effective benefits such as improving customer relationship, better supply management and timely decisions based on real time analytics. In addition, energy companies have also started to use the cloud business model as a source of inspiration for the new energy distribution grids. Security, which has been the headline for many years now remains a huge impediment in the full-scale cloud adoption regardless of the industry.

Insiders represent a greater threat in the context of the energy sector because the ramifications of an attack can cause effects at a state level. As the traditional security solutions continuously fail to detect malicious insiders it becomes more evident that an interdisciplinary approach using psychology could provide better results. AI which usually stands for artificial intelligence has also been named “accelerated intelligence” since cognitive computing can provide insight that would otherwise be elusive, and the result is considerably faster compared to human abilities.

We envision future work towards the refinement of the personality profiling using even cognitive computing technologies to scan psychology papers in order to detect yet uncovered links by current research.

We haven’t addressed the ethical aspects of tapping into the conversations of the employees. Is it ethical to use a machine to read an employee conversation? Is it ethical for a human to read the conversation of another human with its consent? It’s obvious that security and privacy are deeply interweaved [10]. It's easy to see how such a technology could be used by governments to listen to the conversations of its citizens and determine if they develop aversive emotions towards the state. As we explore this dystopian scenario, we should realize that dystopian tools are already deployed in strict regime countries. It’s an embarrassment that the elements that make us human form the biggest enemy of our evolution in terms of society and technology and the result is that we are trying to use technology in ways that sacrifice privacy in order to maintain security. In the context of an increasing use of surveillance technology and artificial intelligence systems, critical areas such as the energy sector will test to the maximum our ability to balance security and privacy.

References

[1] Javied T, Bakakeu J, Gessinger D, Franke J 2018 Strategic Energy Management in Industry 4.0 Environment, *Annual IEEE International Systems Conference (SysCon)*

[2] CA Technologies Insider Threat Report 2018, *CA Technologies*

[3] IBM X-Force Threat Intelligence Index 2018, *IBM Press*

[4] Cost of Insider Threats Report, Ponemon Institute, 2018

[5] Miller H 2016 The Frequency and Impact of Insider Collusion *Community Emergency Response Team (CERT)*

[6] Heidt E and Chuvakin A 2018 Understanding Insider Threats, *Gartner Press*

[7] IBM Personality Insights Guide 2018, *IBM Press*

[8] Eftimie S, Racuciu C 2016 Honeypot system based on software containers, *Mircea cel Bătrân Naval Academy Scientific Bulletin* 2016 Issue 2, pp. 415-418

[9] Navigant Energy Cloud 4.0 2018 *Capturing Business Value through Disruptive Energy Platforms*

[10] Davis B, Whitfield C, Anwar M 2018 Ethical and Privacy Considerations in Cybersecurity, *16th Annual Conference on Privacy, Security and Trust (PST)*