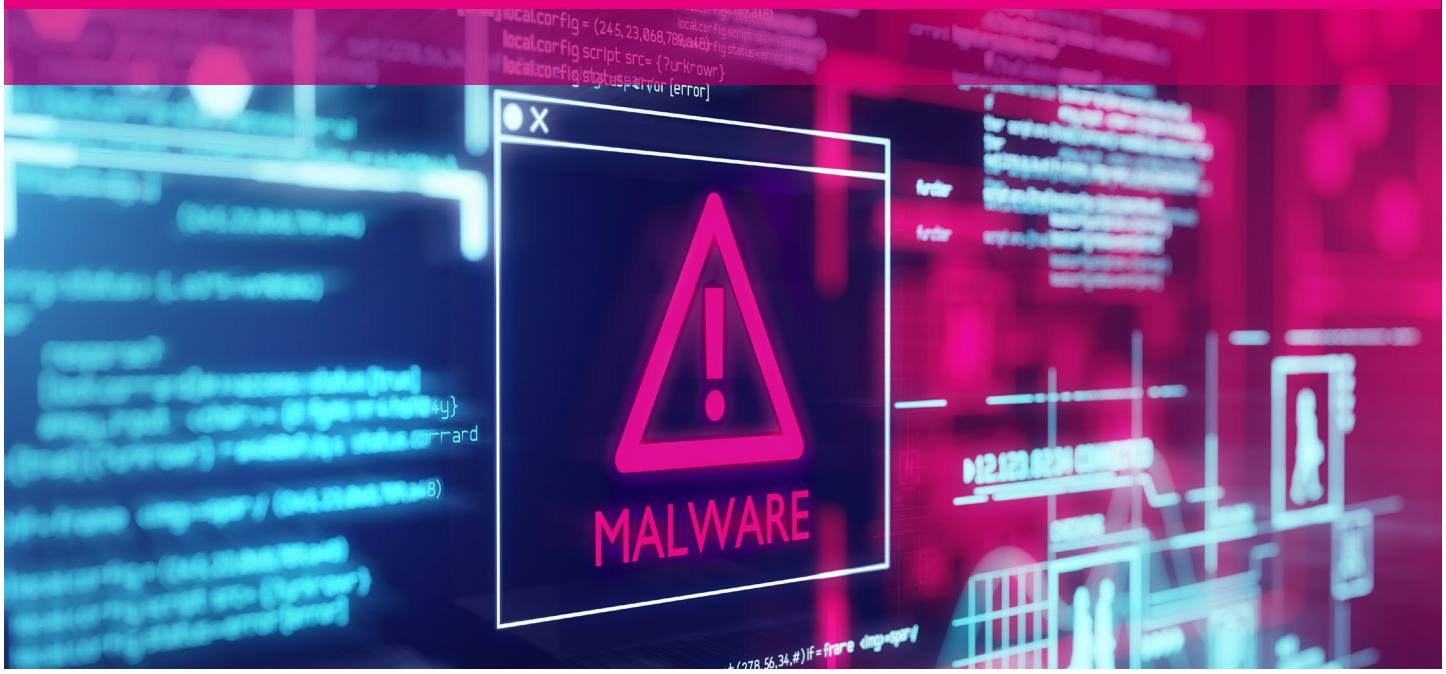
PHISHING DETECTION
MACHINE LEARNING FOR MORE POWERFUL CYBERSECURITY SOLUTIONS



Phishing attacks are among the most prominent and ubiquitous forms of cybercrime. Their volume reaches a staggering 3.4 billion phishing mails per day. Such an amount cannot be handled manually anymore by cyber analysts. Deutsche Telekom is a trusted provider of secure communication services, and it is dedicated to effectively and reliably detecting such attacks. It has specifically designed sophisticated machine learning algorithms to detect features of phishing attempts that are not visible to the human eye – Deutsche Telekom takes phishing detection to a new level.

KEY FACTS:

- Cyberattacks are exploding – the world sees 3.4 billion phishing mails every day
- Efficient and comprehensive detection of such attacks needs to involve automation
- Machine learning algorithms provide the basis for automated phishing detection
- Sophisticated mathematical models reveal tell-tale markers for phishing attempts
- ONAP open source provides the end-to-end orchestration
- Deutsche Telekom's dedicated cybersecurity unit is constantly modernizing its analytics

Deutsche Telekom is a worldwide provider of communication services, it constantly strives to maintain the trust their customers put into it. This entails a comprehensive approach to maintaining cybersecurity.

Among the most wide-spread cybercrime is the so-called phishing – unwarranted digital communication with the apparent air of trustworthiness and familiarity reveals itself to be an attack on sensitive personal data. An email which apparently stems from the family bank entices the recipient to enter their account details into a familiar-looking mask but effectively steals them. A staggering 3.4 billion phishing mails are launched upon internet users every day!

Efficiently detecting and blacklisting these phishing attacks is, therefore, a constant challenge. It is a necessity constantly to adapt to the ingenuity of cyber criminals, i.e. to tune detecting procedures to changing and ever more sophisticated attack patterns. Furthermore, the sheer number of attacks urgently calls for a high degree of automation in the detecting.

With the design of specific machine learning algorithms, Deutsche Telekom provides the basis for automated detection of phishing attacks. Expert domain knowledge and sophisticated mathematical modeling make these machine learning algorithms unique. The character strings of the senders are analyzed and deviations from a suitably defined trustworthiness are detected. In a holistic view of a large numbers of such detector signals, alarms with a high level of confidence are generated.

In close collaboration with Deutsche Telekom's dedicated cybersecurity unit, the presented solution has been achieved as one result of an ambitious joint innovation project with T-Labs. In order to give visitors an impression of the scale and challenge of phishing attacks, Deutsche Telekom has developed a "detection game": Under increasing time pressure, visitors are asked to identify subtle variations to well-established websites. This is precisely what phishing attackers do. After having played the game, visitors will have a good idea of the immensity of the challenge to do the same with a factor of several million!

CONTACT PERSON:

Heiko Lehmann
E-mail: h-lehmann@telekom.de
www.telekom.com

ADDRESS:

Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn, Germany