CybeReady - Simulace phishingu

Kód kurzu: CRE_BLAST

Školení o povědomí o bezpečnosti. Nástroj CybeReady poskytuje komplexní řešení pokrývající všechny vaše potřeby školení kybernetické bezpečnosti s téměř nulovým úsilím v oblasti IT. Nástroj CybeReady, vytvořený odborníky na vzdělávání v oblasti kybernetické bezpečnosti, kombinuje datovou vědu s pokročilou automatizací a umožňuje organizacím provádět snadná, úspěšná a bezproblémová školení.

Simulacemi phishingu trénujete zaměstnance, aby dokázali odhalit phishingové útoky a vyhnout se jim. Obsah se automaticky přizpůsobuje na základě výkonu a umístění zaměstnance (v 38 jazycích). Výsledkem je efektivní, je zaznamenána změna v chování zaměstnanců.

Mminimální odběr je 200 ks licencí.

Obsah modulu

The phishing simulations module allowing to continuously run monthly phishing campaigns, 12 campaings per year. The campaigns are created by the ML engine based on multiple factors: the company's industry, the performances, the size of the company, the locations of employees etc. Each campaign contains a pool of 10 different phishing simulation that the system will use and spread over the month to avoid sending the single same simulation at the same time to all employees. The admin of the system can review in advance the suggested pool of 10 simulations for the next 3 campaigns, re-shuffle, turn off specific simulations or even edit them (not recommended) and then approve them. Once approved, the next 3 campaigns are ensured and will run automatically.

Principy učení

CybeReady has developed a set of learning principles from this starting point to the following principles:

- Learning by doing and knowing the results which allows a person to experience and receive immediate feedback and link their experience to learning. CybeReady has derived sub-principles from this including:
- Just in time and contextual training which connects the failure with the learning content to create a comprehensive learning experience.
- Repetition which is a key to learn and improve.
- Build Cognitive schema which is mental structures that an individual uses to organize knowledge and guide cognitive processes and behavior. People use them to categorize objects and events based on common elements and characteristics and thus interpret and predict the world. If you practice a lot, schema is created automatically in your brain. It enables you to deal with the unknown, with the attack that will happen in the future. This is the reason CybeReady applied the following sub-principles to achieve it:
- Repetition which is a key to let the brain create schema
- Short content that allows the brain to consume quickly and without effort
- Just in time and contextual training, as explained above.
- Build motivation and preserve it assuming that people are not necessarily interested in cybersecurity and learning is a choice, we cannot force an employee to learn. From here CybeReady elaborated the following sub-principles:
- Deliver the content directly to employees (email) without the need to access a different system.
- Short and positive content
- All training content in native language – statistics from research show that learning is much more effective and more engaging in the employee's native language.
- Learning is an individual thing since everyone has a different motivation, a different technical level and background and so needs an adapted training program treated them also with a different risk level.
- The system is expert in training so let it create a tailored program for you. Creating a training program is very complicated since lot of factors should be taken into account (employees' level, languages, locations, days/hours of work etc.)

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- No one should stay behind.
- Risk and adapted program – you are strong as your weakest people. Adapt your program also to your highest risk individuals.

Benefity

Benefits for the security team:

- Data driven recommended programs To save time and also to boost effectiveness, both phishing training and their respective training content are automatically created and tailored to your organization by CybeReady's Machine Learning engine, leaving security teams with the need to only review and approve.
- Adaptive distribution Large organizations find it very challenging to figure out which simulations to send to which employees. CybeReady's Machine Learning engine takes control over simulation distribution, making sure that out of the simulations authorized by the security team only the most relevant are using within every department
- Continuous training mode Creating a security culture requires a security training program that runs year round. Just like hackers work 365 days a year, the training platform should be utilized 365 days a year. The CybeReady solution is built to run continuously – spreading the training across working days and working hours withing each month. By doing so, automatically ensuring that employees are not over trained, that if required non-working days are respected, and that distribution supports creating a cyber culture while reducing IT overhead.
- Risk based training programs Large organizations are continuously faced with the question of how to train high risk groups, given organizational complexities. CybeReady's solution offers an optional data driven approach, by which risk groups are automatically detected and assigned the appropriate training. Risk based programs work both ways, so that employees can both enter and leave the program – based on their own performance.
- Broad language support While only two languages were requested, the key with language support is not how many are supported, but rather in what way are they supported. CybeReady's solution supports every content in the supported languages. This means that from an admin point of view, everything they see is usable, in any requested language – making running a training program very easy, as it's "choose in one language, run in any language". CybeReady supports 40 such languages, German and English included.
- Training program timely communication In most large organizations there are various stake holders involved with the security awareness program. From board of directors, looking to get answers about exposure, to department heads that want to be involved in their employees day to day. The CybeReady solution provides timed reporting for both senior management (automated PowerPoint presentations for the organization or subsidiaries) and mid level managers (monthly emails on their department performance. Reporting is based on advanced risk and operational analytics and is provided in native language.
- Security bites Adapting a security culture in organizations requires making security something employees think about continuously. With CybeReady's security bites, various security topics (selectable from dozens of options) are delivered to employees' inbox in a an engaging and short way that promotes security engagement, thus promoting a security culture.
- Advanced metrics Measuring learning is challenging and most organizations find measuring click rate in phishing simulations a misleading metric. CybeReady's solution provides advanced statistical measures, derived from employee performance to help understand – what is the organizational risk, how are risk trends changing over time, what is the expected performance of a future hire based on historical trends and how does the organization compare to others using the same training methods.

Benefits for Employees:

- Content built for high retention All the content is short, actionable and provided in native language. This method of operation support fast consumption and high retention of content.
- Just in time and contextual training To support the understanding that security training is important but doesn't require too much time, content is provided when it's required (phishing training) or in short intervals (general security awareness training)
- No login required To remove employee friction in the process of learning, all training content are delivered through emails and landing pages

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk