

FRAUD MANAGEMENT

The complexity level of the present IT systems -determined by the wide use of both new and emerging technologies (wireless, VoIP, terrestrial digital technology for TLC, palmtops) and aimed at creating communication business/consumer environments- is now accompanied by a new alarming element: the progress of organized computer attacks with criminal intention to the economic and identity heritage both of individuals and organizations.

This criminal activity is aimed at stealing the user identity and its mimicking in order to steal information or defraud both the user and the company.

The Communication Valley response to online frauds is carried out on two main aspects: *anti-phishing* to minimize the identity theft risk; *transaction monitoring* to block fraudulent activities with identity data obtained in an illegal way.

SCENARIO

Due to the increasing security level of the hardware and software structures of the IT networks of modern companies, the fraudulent intention of individual or group actions is aimed at avoiding the obstacle and –with the help of more devious technologies and social engineering techniques- attacking the most vulnerable point in both houses and companies: the single person, that is either the customer or the operator at his desk.

Fraud is an intentional deceit perpetrated for one's own interests, that is to obtain unauthorized benefits (money, properties and so on) and can refer to legal, commercial, fiscal, currency, sport, food and bank related fields. The term "online fraud" refers to any fraud carried out by using IT tools. For the bank, business, insurance and telecommunication fields, most fraud cases are thefts of identity and mimicking.

SOLUTION

The Communication Valley response to online frauds is carried out on two main aspects:

- anti-phishing to minimize the identity theft risk;
- transaction monitoring to block fraudulent activities with identity data obtained in an illegal way.

ANTI-PHISHING

Phishing is an online fraud technique which uses different methods to mislead the user and convince him to give personal and sensitive information (user name, password, credit card number and so on). The most frequent attacks are carried out through false e-mail messages and suggestions of deceptive links to cheat sites. The attackers are most of the time criminal organizations that expect a very high number of users to be caught in the trap so that they can have the desired information.

Communication Valley fights phishing with a series of proprietary tools specialized in the 24x7 support of its SOC (Security Operations Center) specialists.

The Customer will have access to high service levels (SLA) and leading technologies designed with the aim of providing not only the best anti-fraud service on the market, but also the possibility of continuously evolving the tools created to fight the main existing attack techniques.

The solution of Communication Valley includes the following benefits:

- Preventive analysis of domain registrations in order to identify in advance the domain which could be used for phishing operations
- Detection of phishing attacks 24H thanks to a complete range of tools: bait e-mails, reports by customer and users, "call home" techniques applied to the sites which can potentially be the object of phishing, analysis of web server logs, reports with all the entities dedicated to phishing fight (APWG, PhishTank, CastleCops);
- Analysis of each accident to determine its specific technique;
- Response –aimed at taking down the phishing network- depending on the attack technique and carried out by selecting the specific strategy for each individual strategy;
- Credential dilution and introduction of bait credentials;
- Detailed reports and on-line statistics on the trend of takedown statistics

TRANSACTION MONITORING

The transaction monitoring is a powerful tool to:

- Clearly monitor online activities (both for login and for post-login);
- Identify high risk activities, signal and recommend appropriate actions;
- Enable financial institutions to effectively analyze the activities signaled as high risk;

For online banking operations, it supports many transactions such as:

- Session login;
- Money transfer;
- Profile change;
- Operations on securities;
- Card recharging;

Beside checks for specific bank web applications.

The indicators used by the system and which can increase the risk level during a transaction concern:

- User profile;
- IP profile;
- Device profile.

With a high number of indicators for each profile type, the system defines a risk level to which an action can be associated. Actions can be either a flag on the transaction to activate successive in-depth analysis by the back office or online block, notification and review actions.

REPLY VALUE

Communication Valley has the right competences both for the implementation of a Transaction Monitoring system with its relevant consulting activities on business rules and for the provision of a transaction remote monitoring service.



Within the Reply Spa Group, Spike Reply and Communication Valley are companies specialized in the field of Security and Personal Data Protection.

Reply developed a comprehensive, integrated and consistent offer, in order to tackle any aspect of risks associated to an information system: from detection of threats and vulnerabilities, to the definition, planning and implementation of technological, legal, organizational, insurance or risk retention counter-measures. The Reply mission is to allow its customers to perform their business in a secure environment, thus supporting them during the development and implementation of adequate strategies and solutions, for an effective management of Information Security.

Spike Reply
www.reply.eu