Removing risk from the payments channel

By Andries Kok

31 Mar 2016

Online security breaches are becoming the order of the day, and such incidences are set to rise as the economy comes under increasing pressure. It is, therefore, becoming increasingly important for a business owner to take advantage of risk solutions available in order to safeguard their payment system from vulnerabilities.

Andries Kok

Earlier this month, a breach that affected one of the five major SA banks customers made headlines, and for all the wrong reasons. Bank customers found their accounts illicitly entered into and thousands removed because the one-time pin system didn't work the way it should have.

There are several risks in the payment channel, such as the threat of a data intrusion, the theft of a server, or any other means in which a human intervenes in the system to alter data. Payments to suppliers or staff are also subject to security issues. In fact, the risks to sensitive data such as names, bank account numbers, salaries and addresses will always be at risk.

Security vulnerability

Most payroll and accounting software is username and password access controlled to protect the integrity of the data. Yet, once this software is used to generate output payment files, it usually creates simple data files with no encryption or hashing done to protect the information. This is where the vulnerability lies with these applications and file veracity can be compromised.

By simply accessing this data file, the account numbers and amounts to be paid can easily be modified by an unauthorised staff member or an individual fraudulently accessing the information without anyone noticing. Only once the file has been processed and paid, and it’s too late to do anything about it, will anyone find out that some sort of fraud had been committed.

Many companies are not aware of the risks in the payment channel, or even how to go about plugging the holes.

API technology

Each link in the chain needs to be protected individually to mitigate against unauthorised access. One way of doing this is through a secure Application Programme Interface (API), which connects two applications to each other and ensures that data transfer happens safely. In fact, this way of transferring information, while still relatively new in SA, is becoming increasingly popular due to its high level of security.

PayAccSys has taken this extra security feature on board because its strong algorithms prevent users from interfering with the data. Staying ahead of the curve with API technology is crucial, particularly in the payments industry, where ensuring secure transfer of funds or data is of the utmost importance.

That being said, our advice to other businesses who are considering adopting this new technology to secure data is to ensure that it is designed and managed properly because the API is only as powerful as the code used.

API technology is the way of the future, but remember that it is just one step in the process, a link in the chain which is also dependent on other links being checked and secured in a similar manner.

ABOUT THE AUTHOR

CFO of PayAccSys