CaseStudy

Website Attack Early Warning System

GRED WebCheck JCB Co., Ltd.

SecureBrain

Introduction of website anti-tampering measures to bolster safety of customers accessing own website

JCB

Case Study Company

JCB Co., Ltd.

Founded	January 1961
Capital	10,616.1 million yen
Office	Aoyama Rise Square, 5-1-22 Minami Aoyama, Minato-ku, Tokyo
Business Portfolio	Credit card operations, providing credit card operation services, financing, credit guarantee, collections, issuing of prepaid payment instruments, and sales and its substitution business

Mr. Yusuke Takada,
Vice Chief of the Operation System Supervisory Group in the Operation System Development Department of System Headquarters

The industry's major credit card company, JCB Co., Ltd. (hereinafter referred to as "JCB") introduced SecureBrain's GRED WebCheck, which is a security service to quickly identify and respond to website tampering damage, in January 2010 so as to enhance security for any customers visiting their corporate website by quickly finding and handling such attacks – as they are considered difficult to completely prevent – against a backdrop of increased reports of damage from website tampering.

JCB always seeks out cutting edge security

JCB has been a leader in the credit card industry for half a century as the pioneer in adopting credit card payments for Japanese consumers since its establishment in 1961.

JCB has long been an early adopter of various web-based services (e.g. online The second is "security diagnosis." A comprehensive diagnosis is made by an outsourced specialist company, primarily to assess the response to high-risk threats.

The diagnosis details comply with PCIDSS, and are periodically implemented. As regards the websites efforts to ensure the ultimate safety and convenience, they constantly strive to enhance their security and reliability so that their customers always enjoy safe and worry-free access. subscriptions for credit cards, enquiries about usage amounts and points, and payment requests for utility fees) in a bid to offer its customers the most convenience, and has also long focused on security measures so that customers can use their credit cards safely.

JCB's security response can basically be split into two categories.

The first is "responding in accordance with the latest trends in security threats," or more specifically, security patches for OSes and applications, and in recent cases, responding to threats from which damage can expand rapidly, such as Gumblar.The authentication service, J/Secure ™, and SecureBrain's phishing counteracting tool, PhishWall, were adopted in this regard.

We determine the risks based on information received from security vendors who are business partners, and then responded to as needed.

JCB has always been a step ahead in this industry in terms of being highly security conscious, and is known for its characteristically swift implementation.

Recognition of need for new solutions triggered by Gumblar

JCB had to consider future measures in response to "website tampering."

Mr. Yusuke Takada, Vice Chief of the Operation System

Supervisory Group in the Operation System Development Department of System Headquarters, looked back and commented, “We heard about Gumblar within the last year while hearing about tampering cases that afflicted other companies’ websites, and we became more concerned. Of course, we already have measures in place to protect our system from attack, but cracking technologies keep advancing relentlessly, so we recognized that detection is just as necessary as prevention.”

GRED WebCheck, a product offered by SecureBrain who also provide PhishWall which was installed in 2006, was proposed as a solution around that time.

SaaS-type solution and engine that warrant expectations of high quality prove decisive

The number of news reports detailing damage inflicted by the Gumblar malware had been increasing day by day at the start of 2010, and JCB quickly held discussions about specific measures and the introduction of solutions. JCB also received proposals for other vendor’s products, but deemed them impractical when considering the impact on the system and cost-related issues.

The SaaS-type GRED WebCheck was selected as the primary candidate since it did not impose any additional load on the system.

Subsequently, tests were conducted to check the load on the Website and the influence of any resultant response, but it was confirmed that GRED WebCheck had no problem at all, and service was started immediately.

Having just recently started using a SaaS-type service for the first time, JCB commented, “Being a SaaS model was the primary point for GRED WebCheck. There were no particular concerns with using a SaaS-type product, because the mechanism of GRED WebCheck is detection based on the same processing as general website browsing rather than handing over information to SecureBrain to process.”

Mr. Takada also mentioned some other points regarding its adoption: “We already had a sense of reliability regarding SecureBrain following the introduction of PhishWall, and heard about their stance of accumulating knowhow by providing free security services, so had high hopes concerning the engine, since it was developed based on such knowledge.”

Swift introduction – Hassle-free system proves attractive

It only took about two weeks from first considerations to starting the service.

“Two weeks is much shorter than other security products we’ve used – possibly because this is a SaaS product,” he stated. “Ordinarily, it takes several months to implement systemic changes. When the service actually started, we were relieved that there was no tampering as a result of the checks performed based on SecureBrain’s original analysis algorithm, and there were no difficulty on the management screen on the operational side.” He added that they contacted the support team for enquiries as the detection method and mechanism were unfamiliar for the first month, but ever since then, they have never needed to contact the support team for enquiries, nor had any problems.

The service was quickly introduced thanks to being a SaaS model, and to date, operation has been utterly hassle-free.

This system can be described as very comfortable to use.

JCB focuses on the latest threat trends so as to further improve their security to ensure that customers can visit their corporate website safely and reliably at any time.

At the end of the interview, he added some comments about SecureBrain, the developer of GRED WebCheck, as follows: “We consider SecureBrain to be leaders in the security field, and they have accumulated information unique to SecureBrain. We are happy to further bolster JCB’s security by holding periodic discussions with SecureBrain.”

SecureBrain®

https://www.securebrain.co.jp/eng

About SecureBrain
Based in Tokyo, Japan, SecureBrain
Corporation develop and provide IT
security specializing in cyber security
for web service providers and enterprises.