CaseStudy

Website Attack Early Warning System

GRED WebCheck　CyberAgent, Inc.

SecureBrain

Introduction of WAF alongside website anti-tampering countermeasures Tamper checking + attack blocking to reduce risks

In July 2014, the well-established Internet advertising agency, CyberAgent, Inc. (hereinafter, “CyberAgent”) introduced a SaaS-type website-tampering checking service, “GRED WebCheck,” to their corporate website to prevent damage caused by website tampering in advance, as it is often reported that major company website suffers tampering, and take on a “victimizer” status with any affected users. We asked why CyberAgent changed to GRED from the previously used tampering detection service.

CyberAgent

Case Study Company

CyberAgent, Inc.

Founded	March 18, 1998
Capital	7,203 million yen (As of end of Sep, 2015)
Office	Shibuya markcity West 1-12-1 Dogenzaka Shibuya-Ku, Tokyo
Business Portfolio	Ameba Business Internet Ad Business Game Business Media and Other Business Investment Development Business

CyberAgent Inc.
System Department
Mr. Masatsugu Nishimura

Establishment of IT Security Strategy Office to reinforce security throughout the company

CyberAgent was established in 1998, and has long been a leader amidst the significant changes in the Internet advertising industry, e.g. mail magazines, blogs, and ad technology, as a pioneering Internet advertising agency.

“Information security-related risks” are clearly stated amongst the risk information on their corporate site, and concrete Web security measures are consciously implemented.

On the recruitment side, this company has been proactively recruiting security engineers, and endeavoring to reinforce security not only on their Website, but also in their apps and internal systems.

Under such circumstances, the “IT Security Strategy Office” was established this year. It sets up company-wide security guidelines, boosts security skills and awareness, as well as taking on the role of consultation contact point regarding corporate security.

This office is comprised of ten members, all of whom are “security experts” selected from various departments, such as staff involved in security measures in each department and the person in charge of IT in the sales department.

The members were selected from those responsible or others in a similar position in each department, clearly demonstrating the high priority of security measures in CyberAgent.

In the past, standards for security measures were established by each department, but there was a lack of company-wide standards. Establishment of standards to ensure a certain security level or higher is also one of the objectives of the IT Security Strategy Office.

Inherent vulnerabilities of CMS Using GRED to prevent being victimized by tampering

CyberAgent prioritizes anti-tampering measures as well as focusing on efforts to prevent leakage of personal information held by various services, information about recruitment applicants, and information concerning employees.

As part of this, they took the opportunity afforded to introduce GRED WebCheck – a service that checks for signs of tampering, when renewing their corporate website.

Cloud-type WAF “Scutum” is also introduced, and WAF-based attack blocking and tampering checks are implemented.

The main reason for introducing GRED WebCheck on their static corporate site is the vulnerabilities held by CMS.

Mr. Masatsugu Nishimura of their Company-wide System Office commented on the background to the introduction of GRED: “We use CMS for content management of the corporate website. As long as that is the case, its inherent vulnerabilities are unavoidable, although they are not as serious as those in WordPress, which has many users. Our company is covered on TV and sometimes access surges, so we adopted GRED WebCheck from the viewpoint of minimizing the possibility of damage to tampering to the users and prevent it in advance.”

Improve literacy through internal education as well as systemic defense

Tampering detection had been implemented even before the adoption of GRED, but there were often false detections or malicious script went undetected, and was passed and let through. Following demands for more reliable tampering detection, GRED was introduced by Secure Sky Technology, which operates Scutum.

Were there any other factors besides reliability of detection behind the selection of GRED?

Mr. Nishimura stated: “Their alert specifications for tampering detection matched our image. The mechanism employed by other services we compared was that an alert mail was sent when triggered by any update action. Such a mechanism delivers an alert even for minor updates whenever an update occurs on CMS but splits them up between a number of users. If an alert is output every time a normal update is implemented, the person who checks them may become inured to so many alerts, and so the main concern is that they may be ignored. Under GRED’s specifications, an alert mail is only sent when a malicious update or tampering is detected, so an emergency response can be implemented whenever an alert is received.”

In addition to countermeasures against human error caused by “operational complacency,” the cost and small number of bottlenecks to its introduction, which is unique to SaaS-type models, were also selling points.

CyberAgent’s corporate website has between 15,000 and 20,000 pages, so it can be considered a very expansive corporate website.

Many of these pages are archived press releases. A thousand pages are targeted for checking under the standard GRED service, so Mr. Nishimura’s opinion was as follows.

“Considering the purpose of tampering, which is often virus distribution, pages that are frequently accessed make better targets. Thus, it would be best to apply tampering detection to those URLs that are most often accessed.”

New security issues are unavoidable as Web technology advances.

CyberAgent tackles “Internal education” as one of their countermeasures.

Mr. Nishimura mentioned the mechanism of defense and detection including GRED, and steady measures by CyberAgent to reduce security risks by improving employee literacy.

“Although certain protective measures are in place to counter external cyber attacks by using WAF and checking for tampering, versions of such measures need to be upgraded bearing in mind the risk of more advanced and malicious hacking. In particular, leaks of management information via humans, any resultant account hacking, and internal countermeasures against attacks on the internal network, are issues. Thus, we are promoting the preparation of an internal education environment via e-learning to raise the IT literacy level of our employees.”

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.