【メルマガ＆コラム】Web改ざん対策と改ざんされた場合の自動復旧について

■ ネクスト・イットNEWS Vol.19
2011/03/04

いつもお世話になっております。
ネクスト・イットの吉政でございます。

インプレス社クラウドWatchの記事によると、2009年12月以降、Webページが改ざんされたことを発表している主な企業は、ラジオ関西、ホンダ、JR東日本、信越放送、ローソン、ハウス食品、モロゾフ、京王グループなどで、いずれも、Gumblarの亜種によるものと思われる改ざんがあり、ウイルス感染を広げるためのスクリプトが埋め込まれたようです。

Web改ざんは日本国内でも数日に1件発生しているといわれています。

これらの有名企業でまったく防止対策が施されていなかったとは思えません。
恐らくですが、何らかの防止対策がされていたにも関わらず、 Web改ざんがされたのではないかと思います。　もし、そうであれば、皆さまのサイトでも防止対策だけでなく、万が一の改ざん後の対策も必要なのではないかと思います。

そこで、弊社では日本国内官公庁を中心に300サイト以上の実績があるWeb改ざん監視＆改ざん後の自動復旧ソリューション「WebALARM」の開発元であるe-lock社から技術者を招き、「WebALARM」の解説セミナーを開催します。

Web改ざんの監視、自動復旧に興味がある方は是非この機会にご参加ください。

※本セミナーの詳細は以下をご覧ください。
http://nextit.jp/seminar/WA0316.html

それでは、今号も宜しくお願いいたします！

―目次―

―詳細と解説―

【1】セミナー関連

■第6回データセンタ向けOpen-Xchangeセミナー（3月24日東京開催）

急速に発展するクラウドコンピューティング、モバイル化時代への対応策として、社内情報伝達の確実性、共同作業最小限のツール整備が急務となりつつあります。Open-Xchangeは、企業が最小限必要としているメール機能、ドキュメント共有等を一括に、スムーズにて簡単にコストパフォーマンスを実現したグループウェアです。
このセミナーでは、Open-Xchangeの効果的な運用方法を、技術解説やデモンストレーションやQ&Aセッションを交えてご説明します。

【第6回：3月24日開催】
詳細は⇒ http://nextit.jp/seminar/ox0224.html

■最新Web改ざん対策セミナー（3月16日東京開催）

日本国内でも数日に1件発生しているといわれているWeb改ざんの被害。自社のWebサイトがダウンしていたり、悪性のウィルスを自社サイトから撒き散らし

てしまっては会社としての信頼を失いかねません。
本セミナーでは、日本国内官公庁を中心に300サイト以上の実績がある「WebALARM」の開発元であるe-lock社から技術者を招き、「WebALARM」デモ＆解説セミナーを開催します。Webコンテンツの監視、自動復旧に興味がある方は是非この機会にご参加ください。

詳細は⇒ http://nextit.jp/seminar/WA0316.html

【2】戦略コラム

■【第十回】Web改ざんの被害例

今回はWeb改ざん対策特集と言うことで、Web改ざんについての判例も紹介してみたいと思います。

メルマガの冒頭で2009年12月以降、Webページが改ざんされたことを発表している主な企業は、ラジオ関西、ホンダ、JR東日本、信越放送、ローソン、ハウス食品、モロゾフ、京王グループなどで、いずれも、Gumblarの亜種によるものと思われるWeb ページの改ざんがあったことをお伝えしました。以下では、別件ではありますが、Web改ざんの被害イメージが分かるものをご紹介します。

◆　2010年3月

==========
三菱電機のサイトに不正アクセスがあり、
顧客情報など約1万1000件が流出した可能性。
==========
対象：三菱電機のWebサイト「DIAX-NET」と「MELLASER- NET」
対象サイトへ不正アクセスがあり、会員登録していた顧客情報などが流出した可能性があることがわかったそうです。
想定被害数：1万1384件の個人情報が漏洩。
==========

個人情報が漏洩した場合、過去の判例を見ても2-3万円/人と言うことも珍しくなく、仮に2万円で計算しても、約2億3千万円の被害額をイメージできます。さらに、その信用や株価などの下落を考えると、相当大きなダメージになることは容易に想像がつきます。

◆　2010年1月

==========
検索サイト「Mooter」が改ざん、検索窓設置サイトにも影響。
==========
対象：検索ウェブサイト「Mooter」
被害状況：「Adobe」関連の未修正の脆弱性を攻撃する不正なJavaScriptが埋め込まれたそうです。同社の「検索窓」を設置しているWeb運営者、および設置された検索窓で検索を実施したWeb閲覧者にウイルス感染のおそれがあるそうです。
==========

Web検索エンジンのような競合が多いWebサービスでは顧客の離脱も速いと思います。その状況の中でこのような改ざん事件は非常に大きな損害になると思います。

そのシステム責任者が会社の中でどのような処罰を受けたか分かりませんが、表ざたになってしまえば、何らかの処罰があってもおかしくはないと思います。情報システム責任者としてはWeb改ざん防止対策を施すと同時に万が一の際に被害を最小限にとどめる「WebALARM」のような仕組みを導入しておくことが重要であると改めて思いました。

※「WebALARM」については以下のサイトをご覧ください。
http://nextit.jp/product/webalarm/index.html

（吉政　忠志）

編集後記

SourceForge.JPを利用している人はご存知かと思いますが、実はOpen-XChangeの日本語化プロジェクトを公開しようと準備をしています。コンテンツはオイオイですが順次公開してまいりますので、是非ご期待ください。（吉政）

==========
メール配信元：ネクスト・イット株式会社　「ネクスト・イットNEWS」編集部
発行人：営業推進本部　谷尾　真人
編集人：マーケティングアドバイザー　吉政　忠志
東京都品川区南品川2-4-5NAビル　TEL:03-5783-0702　FAX：03-5783-0734
URL:http://nextit.jp/　MAIL：info@nextit.jp
==========
※今後、弊社からのご案内が不要の場合は、誠に恐れ入りますがこのメールの返信で『ご案内メール不要』のご連絡をいただきますよう、宜しくお願い申し上げます。