— ＡＵＳ（アルテミス・ユーザ・サポート）便り 2016/01/25号 —

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●北海道大学サーバに不正アクセスか･･･個人情報11万件流出の可能性も

http://www.itmedia.co.jp/news/articles/1601/13/news123.html
http://mainichi.jp/articles/20160114/ddr/041/040/005000c

このニュースをザックリ言うと･･･

- 1月13日（日本時間）、北海道大学より、大学内のサーバが不正アクセスを受けた可能性があるとの発表がありました。

- 発表によれば、問題のサーバは同大学生の就職支援を行うキャリアセンターのファイルサーバで、「昨年末に大量のスパムメールを送信していたこと」また「ログ等の調査から不特定多数の外部サーバと通信を行っていたこと」が確認され、ネットワークから切り離されたとのことです。

- 当該サーバには在学生約18,000人・卒業生約95,000人および企業約2,000社、合計で約11万件の個人情報・法人情報が保存されており、これらも流出した可能性があるとして調査中ですが、現時点では実際に流出したかは不明で、流出による被害は確認されていない模様です。

AUS便りからの所感等

- 当該サーバは外部から接続できないよう設定され、アクセス権限を持つのも少数の職員のみだったとのことですが、それでもこういった問題が起きたことについては、例えばその職員の誰かが標的型攻撃を受け、利用しているPCが踏み台にされた等の可能性が考えられます。

- 一方で、実際に個人情報等が流出したかについてまでは確認されていないものの、内部で問題が発生していたことを把握できたのは、サーバやネットワークの監視体制がある程度整っていたことによるものと言えるでしょうが、そうでなければ、気付かれないうちに別のサーバにも侵入されるなど、被害はより大きくなっていた恐れもあります。

- 標的型攻撃を行うようなマルウェアに感染しないために各PCにアンチウイルスを導入すること、あるいはマルウェアが侵入しようとしていた、さらには感染して外部へ通信しようとしていた、等の問題の発生を的確に突き止めるために、要所要所にUTM等を設置することが重要でしょう。

ITmedia ニュース

2016年01月13日 17時35分 更新

北大に不正アクセスの疑い　在学生・卒業生ら約11万件の情報流出か

北海道大学のサーバが不正アクセスを受けた可能性があり、在学生・卒業生の個人情報を含む約11万件の情報が流出したおそれがある。

[ITmedia]

北海道大学は1月13日、就職活動支援などを行う「キャリアセンター」のサーバが不正アクセスを受け、在学生と卒業生、企業など計約11万件の個人・法人情報が流出した可能性があると発表した。

同大によると昨年末、大量のスパムメールを送信したことで自動的にこれを遮断したサーバが学内に見つかった。このサーバはキャリアセンターのファイルサーバであることが分かり、ログなどを調べたところ、不特定多数の外部サーバと通信していることが今月4日に判明。サーバをネットワークから切り離した。

同サーバには在学生約1万8000人・卒業生約9万5000人と企業約2000社、合計計約11万件のデータが保存されており、流出した可能性があるとして調べている。現時点では流出による被害は確認されていないという。学内のほかのサーバについても調査する。

情報が流出した個人・法人には説明と謝罪の書簡を送る。同大は「職員に対してはより一層，個人情報の適正な管理の徹底を図り，再発防止に努めてまいります」としている。

毎日新聞

個人情報
北大に不正アクセス　11万件流出か

毎日新聞 2016年1月14日 北海道朝刊

北海道大は13日、学内のサーバーが不正アクセスされ、全在校生ら約11万3000人の氏名や住所、生年月日など個人情報が流出した可能性があると発表した。北大は調査委員会を設置し、道警札幌北署に通報した。情報の不正利用などは確認されていないという。

北大によると、学生の就職支援を行うキャリアセンターのサーバーが先月27日、学外に約500件の迷惑メールを一斉送信。翌28日に気付き調査したところ、海外を含めた不特定多数のサーバーと通信していたことも今月4日に判明した。何者かがパスワードを不正入手し、侵入した可能性もあるという。

北海道大学 HOKKAIDO UNIVERSITY

情報セキュリティインシデント（不正アクセスの疑い）について

平成28年1月13日
北海道大学

昨年12月27日，大量のスパムメールが送信されたことにより，自動的にメールの送信を遮断したサーバがあることを，12月28日に確認しました。
その後，当該サーバが本学キャリアセンターのファイルサーバであることが判明し，ログ等の調査・確認を行い，1月4日に当該サーバが不特定多数の外部サーバと通信していることが判明したため，当該サーバをネットワークから切り離す措置を講じました。

●「最悪なパスワード」2015年版ランキング発表

http://nlab.itmedia.co.jp/nl/articles/1601/20/news071.html

このニュースをザックリ言うと･･･

- 1月19日（現地時間）、スマートフォン向けパスワード管理ツールなどを提供する米SplashData社より、インターネットで多用されている「最悪なパスワード」2015年版ランキングが発表されました。

- 最も多かったのは、昨年と同じく「123456」、続いてトップ5として「password」「12345678」「qwerty」「12345」が続いていますが、これらも相互に多少の順位変動はあるものの昨年と同じという結果になりました。

AUS便りからの所感等

- ランキングで挙がっているトップ25のパスワードは、「簡単な数字の羅列」「英単語(かつアルファベット小文字のみ)」「キーボードで左から順にタイプしたもの」といった特徴があり、アカウント奪取を目論む攻撃者であれば真っ先に試行するであろうパスワードです。

- 現在では多くのサービスにおいて、あまりにも簡単なパスワードを設定していないかチェックを行うようになっていますが、そのチェックを回避可能な、依然破られやすい簡単なパスワードを設定するユーザもいるようです。
（例えば、「password」が設定できないところ、「Password1」で登録する等）

- どういったパスワードを設定するか、パスワードを如何に管理するかは長年議論となっていますが、とにかくすぐに推測されてしまうパスワードを設定しないことがまずは第一です。

「最悪なパスワード トップ25」(カッコ内は前年順位)
● 1:123456（1） ● 2:password（2） ● 3:12345678（4） ● 4:qwerty（5） ● 5:12345（3） ● 6:123456789（6） ● 7:football（10）
● 8:1234（7） ● 9:1234567（11） ●10:baseball（8） ●11:welcome（New） ●12:1234567890（New） ●13:abc123（14）
●14:111111（15） ●15:1qaz2wsx（New） ●16:dragon（9） ●17:master（19） ●18:monkey（12） ●19:letmein（13） ●20:login（New）
●21:princess（New） ●22:qwertyuiop（New） ●23:solo（New） ●24:passw0rd（New） ●25:starwars（New）

ねとらぼ

●ゾーン転送設定に注意、BINDは新たな脆弱性へのパッチ適用を

http://internet.watch.impress.co.jp/docs/news/20160112_738569.html

このニュースをザックリ言うと･･･

- 1月12日（日本時間）、セキュリティ専門機関JPCERT/CC等より、自ドメインの情報を提供する権威DNSサーバにおいて「ゾーン転送」に関する不適切な設定がされているケースがあり、第三者にホスト名とIPアドレスの一覧が流出する可能性があるとして、設定を見直すよう注意喚起が発表されました。

- また1月20日（日本時間）には、DNSサーバソフト「BIND」について2件の脆弱性（CVE-2015-8704, CVE-2015-8705）が発表され、開発元の米ISCより修正バージョン（BIND 9.10.3-P3/9.9.8-P3）がリリースされています。

AUS便りからの所感等

- ゾーン転送は、複数のDNSサーバ（マスター・スレーブ）でDNSレコードを共有するよう、スレーブサーバがマスターサーバからゾーン情報をコピーするために使われるものですが、設定が不十分な場合、任意のアクセス元からゾーン転送リクエストを受け付ける可能性が指摘されており、ゾーン転送を使用している場合は、マスターサーバ側がスレーブサーバのあるIPアドレスからのみゾーン転送を許可するようになっているか確認すべきでしょう。

INTERNET Watch


ニュース
権威DNSサーバーの設定不備でゾーン情報流出、設定の再確認を
(2016/1/12 18:15)
G+1 8 B! 20 ツイート リスト いいね！ シェア 71 Pocket 72
権威DNSサーバーの設定不備によるゾーン情報流出の危険性について、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）や株式会社日本レジストリサービス（JPRS）、一般社団法人日本ネットワークインフォメーションセンター（JPNIC）が12日、注意喚起を出した。管理者に対して設定の再確認を呼び掛けている。
アクセスコントロールが適切に設定されていないために、必要なIPアドレス以外からのゾーン転送要求に応答し、第三者にホスト名とIPアドレスの一覧が流出してしまうというもの。こうした情報が悪意の第三者に流出すれば、その情報に基づいたポートスキャンの実行、ネットワーク構成の推測、サービス提供形態の分析など、潜在的な脅威の増加につながる危険性があるとしている。

- BINDの脆弱性は、悪用されることでDNSサーバがダウンし、外部から自組織のドメイン名を引くことができなくなる可能性があり、即ち自組織のWebサイトやメールサーバへアクセスできなくなることにつながる可能性があります。

- BINDについては昨年下半期以降7月・9月・12月と特に更新の頻度が増えていますので、Linuxディストリビューションのパッケージにしろ、独自にコンパイルしている場合にしろ、常時速やかにアップデートできる体制を整えられているかが肝心であり、また、不正なDNSパケットに関しては、UTMの設置によって防御できる可能性もあります。