مرکز مدیریت راهبردی افتا

جمهوری اسلامی ایران
ریاست جمهوری

شماره: ۰۲/۹۲۸۹/الف/ع
تاریخ: ۱۴۰۲/۱۲/۱۳
پیوست: دارد

آنی

تمامی دستگاه‌های اجرایی کشور (دارای زیرساخت حیاتی)

موضوع: دستورالعمل امن سازی اضطراری

باسلام و احترام

با توجه به برآوردهایی که از احتمال وقوع حملات سایبری می‌شود و نقاط ضعفی که در اغلب حملات اخیر مورد سوء استفاده قرار گرفته‌اند لازم است تمامی دستگاه‌های زیرساختی با قید فوریت نسبت به اجرای دستورالعمل امن‌سازی اضطراری پیوست اقدام نمایند.

انصاری
رئیس مرکز

رونوشت:

- جناب آقای دکتر آقامیری دبیر محترم شورایعالی و رئیس مرکز ملی فضای مجازی برای استحضار
- رئیس محترم سازمان حراست کل کشور برای استحضار

آدرس: تهران- خیابان شهید بهشتی- خیابان قائم مقام فراهانی- کوچه شهدا- پلاک ۱ و ۳- تلفن: ۴۳۴۳۹۰۰۰ فاکس: ۸۸۷۱۳۲۳۵ صندوق پستی: ۷۱۷۸-۱۵۸۷۵

دستورالعمل امن سازی اضطراری

۱- تعداد کاربران دارای دسترسی‌های مدیریتی (ادمین) را به حداقل برسانید و به صورت مستمر آن‌ها را کنترل نمایید.

۲- رمز عبور تمام کاربران دارای دسترسی‌های مدیریتی (ادمین) به ویژه مدیران دامنه (دامین ادمین‌ها)، با فوریت تغییر داده شوند.

۳- برای حذف تیکت‌های طلایی (گلدن تیکت‌ها) رمز عبور حساب کاربری KRBTGT در اکتیو دایرکتوری را دو مرتبه پشت سر هم تغییر دهید.

۴- رمز عبور تمامی کاربران دارای دسترسی‌های مدیریتی محلی (لوکال ادمین‌ها) را تغییر دهید.

۵- از حداقل بودن دسترسی‌های حساب‌های کاربری مورد استفاده برای دسترسی به وب‌سرورها و دیتابیس‌ها اطمینان حاصل کنید.

۶- پس از بررسی و اطمینان از جایگزین نمودن موارد احتمالی استفاده از سازوکار Digest authentication در سطح شبکه با قید فوریت نسبت به غیرفعال سازی این روش احراز هویت بر روی سیستم‌های ویندوزی اقدام نمایید. مراحل زیر در نسخه‌های ویندوز ۷، ویندوز ۸، ویندوز سرور ۸، ویندوز ۲۰۰۸ آر ۲ و ویندوز سرور ۲۰۱۲ قابل اجرا است:

۶-۱- نصب وصله شماره ۲۸۷۱۹۹۷KB شرکت مایکروسافت

۶-۲- تنظیم رجیستری:

```
reg add
HKLMSYSTEMCurrentControlSetControlSecurityProvidersWDigest /v
UseLogonCredential /t
REG_DWORD /d 0
```

۶-۳- نکته: در نسخه‌های جدید ویندوزهای کلاینت و سرور، نیاز به نصب پچ نیست و به صورت پیش‌فرض مقدار کلید صفر است ولی باید بررسی کنند که تغییر نکرده باشد و اگر بر روی ویندوزهای جدید مقدار ۱ شده بود و خود سازمان این اقدام را انجام نداده بود، احتمالاً سیستم هایجک شده است:

```
reg query
HKLMSYSTEMCurrentControlSetControlSecurityProvidersWDigest /v
UseLogonCredentia
```

۷- استفاده از قابلیت SMB NTLM Blocking برای جلوگیری از اتصالات SMB مبتنی بر NTLM برای جلوگیری از سرقت هش رمزهای کاربران

۷-۱- مسدودسازی به صورت جنرال (پیشنهاد می‌شود برای جلوگیری از خطای انسانی از group policy استفاده کنند) و در موارد خاصی که نیاز است (که ترجیحاً نباشد) باید لیست exception قرار دهند، اما دقیق با تعریف آدرس IP، مقدار DNS یا netbios name ماشین مقصد که پیشنهاد می کنیم آدرس IP ست کنند. چون ممکن است به دلیل زیر به اکسپشن لیست نیاز داشته باشند:

This allows an administrator to configure a general block on NTLM usage while still allowing clients to use NTLM for specific servers that do not support Kerberos, either because they are not Active Directory domain joined or are a third party without Kerberos support.

۷-۲- نحوه مسدودسازی به کمک گروپ پالیسی:

To configure SMB NTLM blocking for the entire Windows machine, enable the group policy under:

Computer Configuration \ Administrative Templates \ Network \ Lanman Workstation \ Block NTLM (LM, NTLM, NTLMv۲)

برای تعریف لیست exception باید در بخش زیر و در هر ردیف آدرس IP سرور مقصد درج شود:

To configure SMB NTLM blocking with exceptions for certain remote devices, enable the group policy under:

Computer Configuration \ Administrative Templates \ Network \ Lanman Workstation \ Block NTLM Server Exception List