Da: noreply@istruzione.it
Oggetto: URGENTE - CSIRT MI - Alert Phishing 29/12/2020
Data: 29/12/2020 17:06:07

Gentile Utente,

si segnala in queste ore un'intensa azione di tentativi di phishing ai danni del Ministero dell'Istruzione.

Tali messaggi sono indirizzati a caselle di posta elettronica istituzionali, provenendo da mittenti 'verosimili', interni o esterni all'Amministrazione, e rispetto ai quali nei testi si richiede di scaricare o aprire file che sono in realtà virus in grado di recare grave infezione alle postazioni di lavoro utilizzate e, a cascata, pregiudizio sull'infrastruttura tecnologica del MI.

Per quanto i mittenti possano essere noti, il messaggio può dunque essere malevolo.

Si può riscontrare tale evidenza passando il puntatore del mouse sul nome dello stesso mittente e verificando eventuali anomalie nell'indirizzo mail visualizzato (disallineamento con il nome visualizzato, stringhe alfanumeriche complesse o non interpretabili nel nome utente, dominio estero, ecc).

Non si devono assolutamente aprire tali file in allegato.

Qualora ciò fosse stato fatto, occorre procedere immediatamente alla scansione della postazione di lavoro utilizzata e, subito dopo, provvedere al cambio delle credenziali di tutti gli account utilizzati a fini lavorativi (la stessa posta elettronica, accesso al sistema informativo dell'istruzione, …).

In alcuni casi, si potrebbe avere già certezza della mail malevola, sempre da non considerare assolutamente o darvi seguito, qualora si ritrovasse in allegato un file di testo denominato '*Malware Alert Text.txt*'; tale riscontro significherebbe che i sistemi di protezione del sistema informativo del Ministero sono riusciti ad intercettare l'attacco.

**

Non solo nella situazione della segnalazione in oggetto, bensì sempre, qualora doveste incorrere in messaggi mail del suddetto tipo, allo scopo di limitare l'occorrenza di incidenti di sicurezza, si devono seguire le seguenti raccomandazioni.

- non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungano da caselle di posta non note;
- non installare software sulle proprie postazioni di lavoro, soprattutto se a seguito di sollecitazioni via e-mail;
- non dare seguito alle richieste di e-mail sospette;
- nel caso in cui la richiesta provenga da parte del personale tecnico dell'Amministrazione, verificare attentamente il contesto: *l'e-mail era attesa? Le frasi sono scritte con grammatica corretta? Il software da installare ha un fine specifico? Eventuali link nell'e-mail puntano a siti conosciuti? Il mittente è corretto?*

Inoltre si ricorda di:

- scansionare periodicamente per la ricerca malware le postazioni di lavoro ed i dispositivi utilizzati per lavoro;
- nel caso di utilizzo del PC personale (telelavoro/smart working) assicurarsi periodicamente:

- che il sistema operativo della propria postazione di lavoro sia aggiornato;
- che la propria postazione di lavoro sia dotata di antivirus e che questo sia aggiornato per una periodica scansione;

- che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che, al momento della modifica, non siano apportate solo piccole modifiche (come ad esempio numerazioni progressive ...)

Si ricorda inoltre che nell'area riservata intranet allo CSIRT MI (dopo il login, sezione: *Area Riservata > Computer Security Incident Response Team > Security Awareness*) sono presenti i contenuti relativi a campagne malevole di phishing in corso ed aggiornamenti su nuovi virus che potrebbero infettare le postazioni di lavoro del personale della Pubblica Amministrazione.

E' fortemente consigliata la lettura dei suddetti contenuti, allo scopo di tenersi aggiornati sui rischi

informatici incombenti sull'Amministrazione e proteggere sia la propria operatività sia il patrimonio informativo del Ministero da possibili attacchi.

Per completezza, si allegano alla presente mail le Raccomandazioni dello CSIRT MI per la sicurezza.

Inoltre, ai fini tutela delle informazioni riservate di lavoro, ivi inclusi i dati personali propri e di terzi, si raccomanda fortemente di non lasciare mai il personal computer di lavoro incustodito o comunque non sotto il proprio diretto controllo (e.g. computer lasciato in bagagliaio auto in propria assenza).

**

Grazie della collaborazione

CSIRT MI