UNIMORE

UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

RACCOMANDAZIONI DI SICUREZZA INFORMATICA

Giugno 2019

A cura del Gruppo CoreMMS

Progetto “Transizione al digitale” approvato dal CdA del 21/12/2018
Sottoprogetto “Applicazione Misure Minime di Sicurezza in Ateneo”

SOMMARIO

INFORMAZIONI GENERALI SULLA SICUREZZA INFORMATICA IN ATENEO

Per garantire la sicurezza della rete di Ateneo e dei sistemi informatici tutti gli **Utenti** (docenti, ricercatori, personale Tec-Amm, collaboratori, studenti, dottorandi) che utilizzano una postazione di lavoro collegata alla rete Unimore devono adottare le Misure Minime di Sicurezza (MMS) richieste dalla circolare AgID (Agenzia per l'Italia Digitale) del 18 aprile 2017 n. 2/2017.

https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Tra l'altro, le MMS obbligano alla riservatezza delle password, all'utilizzo di un software antivirus/antimalware aggiornato, all'installazione di solo software autorizzato e all'aggiornamento costante del sistema operativo e degli applicativi in uso.

Gli Utenti sono invitati a rivolgersi ai **referenti informatici della propria struttura** (elenco alla pagina http://www.sia.unimore.it/site/home/referenti-informatici.html) per informazioni tecniche e segnalazioni di abuso e a verificare periodicamente tutte le raccomandazioni di sicurezza indicate dalla propria struttura di afferenza e quelle pubblicate sul sito http://www.sicurezzaict.unimore.it .

In particolare, tutti gli utenti sono invitati a leggere e seguire quanto indicato di seguito nelle "RACCOMANDAZIONI DI SICUREZZA PER TUTTI GLI UTENTI".

Gli Utenti che possono amministrare dispositivi informatici perché a conoscenza di credenziali con diritti di super-utente/administrator sono considerati *amministratori di sistema* di tali dispositivi (postazioni di lavoro e ambienti server) e devono seguire le ulteriori indicazioni "RACCOMANDAZIONI DI SICUREZZA PER AMMINISTRATORI DI SISTEMA".

Le MMS richiedono l'utilizzo di configurazioni sicure standard per la protezione dei sistemi operativi (ABSC ID 3.1.1 3.2.1). Pertanto, per l'installazione e configurazione di un ambiente server seguire le indicazioni "RACCOMANDAZIONI DI SICUREZZA PER LE INSTALLAZIONI DI SERVER".

Analogamente, per le stampanti e le multifunzioni collegate in rete, seguire le indicazioni "RACCOMANDAZIONI DI SICUREZZA PER STAMPANTI".

Per i casi d'uso non previsti dalle MMS di Ateneo e dal presente documento, gli Utenti possono fare riferimento al documento *"Linee guida per la configurazione per adeguare la sicurezza del software di base"*, pubblicate sul sito di Agid, nel quale sono riportate le best-practice per la corretta gestione dei sistemi informatici nella Pubblica Amministrazione.

RACCOMANDAZIONI DI SICUREZZA PER TUTTI GLI UTENTI

Le raccomandazioni di seguito valgono per tutti gli utenti che utilizzano dispositivi collegati alla rete Unimore.

- Impostare password complesse e cambiarle frequentemente
- Conservare tutte le proprie password in modalità sicura e protetta, non scriverle su fogli o post-it, non comunicarle a voce o via email ad alcuno
- Cambiare immediatamente una password che è stata per qualche motivo comunicata a terzi o che si sospetti abbia perso il requisito di segretezza
- Evitare di salvare la password di un servizio sul browser o su un'applicazione ma digitarla sempre ad ogni nuovo accesso
- Impostare sempre uno screen-saver con richiesta di password o altro meccanismo di sicurezza (es. utilizzare l'opzione "Blocca" in Windows che rimanda alla schermata di login senza disconnettere) per proteggere l'accesso alla propria postazione di lavoro nel caso di assenza anche temporanea
- Quando possibile, spegnere la postazione di lavoro al termine dell'attività lavorativa giornaliera
- Assicurarsi che sia presente un antivirus/antimalware aggiornato su tutte le proprie postazioni di lavoro per evitare la diffusione di virus in rete
- Effettuare la scansione con l'antivirus dei file e dei supporti provenienti dall'esterno
- Assicurarsi che il sistema sia continuamente aggiornato, installare le ultime patch di sicurezza del sistema operativo e del software installato
- Nel caso di utilizzo di client di posta elettronica, configurarlo in modo che non apra automaticamente gli allegati
- Prestare attenzione a messaggi di posta elettronica sospetti, di cui non si conosce il mittente e/o che contengono link sospetti o allegati non richiesti, non aprire gli allegati, non seguire i link (vd. http://posta.unimore.it/attenzione-al-phishing/)
- Disattivare l'anteprima automatica dei contenuti dei file
- Disattivare l'esecuzione automatica di contenuti dinamici (es. macro) presenti nei file
- Segnalare ogni sospetto furto di credenziali, rilevamento virus, tentativo di intrusione o altro abuso ai referenti informatici di struttura
- Fare sempre riferimento ai referenti informatici di struttura per l'installazione e la configurazione di nuovi dispositivi

RACCOMANDAZIONI DI SICUREZZA PER AMMINISTRATORI DI SISTEMA

Le raccomandazioni di seguito sono rivolte a chi ha accesso con diritti amministrativi / super-utente ad uno o piú dispositivi (computer, portatili, server, stampante di rete, etc) collegati alla rete Unimore.

- Attenersi a quanto indicato nelle "RACCOMANDAZIONI PER TUTTI GLI UTENTI"
- Preferire sempre l'utilizzo di credenziali personali che non abbiamo privilegi di amministratore per l'utilizzo ordinario del proprio computer
- In caso sia necessario utilizzare privilegi di tipo amministrativo di frequente per effettuare operazioni di installazione/aggiornamento/configurazione del sistema, includere il proprio account nei gruppi di amministratori di dominio o locali in caso di sistemi Windows, o includere il proprio account nel gruppo dei *sudoers* per i sistemi Linux/Unix e MacOS
- Se sono configurate credenziali di default nel dispositivo e negli applicativi, provvedere a modificare subito la password
- Se è necessario autorizzare più profili amministratore, mantenere l'elenco delle utenze amministrative. Ogni *credenziale* deve essere nominativa e riconducibile ad una sola persona
- Se la postazione è utilizzata da più utenti, ove possibile, non creare utenti locali ma abilitare l'accesso tramite il "Servizio di directory" di UniMORE (per es. LDAP, Active Directory, Shibboleth, ecc.)
- Quando possibile, consentire l'accesso solo a utenti identificati nel sistema di identity management di Ateneo ed eliminare i profili utente non necessari o dismessi
- Utilizzare password complesse per l'utenza amministrativa, di almeno 14 caratteri e cambiare la password frequentemente (es.ogni 6 mesi). Al posto della password è possibile utilizzare un meccanismo di autenticazione più forte (chiavi ssh, certificati digitali, etc)
- Adottare misure di custodia e protezione adeguate per garantire la disponibilità e la riservatezza della password dell'utenza amministrativa in caso di necessità
- Non utilizzare la stessa password per utenze o servizi diversi
- Non comunicare le proprie password ad alcuno
- Evitare di salvare le password sul sistema operativo o su applicativi in uso
- Aggiornare costantemente sia il sistema operativo sia le applicazioni installate alle ultime versioni senza vulnerabilità note e alle ultime patch di sicurezza disponibili
- Installare un antivirus/antimalware e tenerlo costantemente aggiornato
- Installare un firewall locale
- Installare solo software autorizzato dalla propria struttura e, nel caso di particolari esigenze, comunicare l'eccezione ai propri referenti informatici che inseriranno il

software nella lista degli autorizzati e valuteranno se sono necessarie particolari misure di sicurezza

- Disabilitare il boot da rete, USB, dispositivi rimovibili, impostando una password per il BIOS e per la modifica del dispositivo di boot
- Abilitare solo le condivisioni in rete necessarie all'attività lavorativa e protette mediante l'utilizzo di credenziali di accesso
- Per l'eventuale amministrazione da remoto utilizzare solo canali di comunicazione sicuri
- Trasferire file solo in modo cifrato (SCP, SFTP, FTPS, Rsync Over SSH)
- Effettuare almeno settimanalmente e su sistema esterno una copia di sicurezza delle informazioni strettamente necessarie per il completo ripristino del sistema
- Nel caso in cui la postazione di lavoro contenga dati con particolari requisiti di riservatezza, sensibili o strategici, impostare la cifratura del disco se permessa o applicare la protezione crittografica
- In caso di dismissione di una postazione di lavoro, disinstallare il software con licenza installato e cancellare le informazioni contenute nel disco se non cifrate con password

RACCOMANDAZIONI DI SICUREZZA PER LE INSTALLAZIONI DI SERVER

Per l'installazione e la configurazione del sistema operativo gli utenti che gestiscono proprie postazioni di lavoro o ambienti server devono seguire queste raccomandazioni:

- evitare l'uso di sistemi preinstallati di cui non si conosce in dettaglio la configurazione, se si usano immagini virtuali o preconfigurazioni modificare le credenziali di amministratore prima di collegare il sistema alla rete
- se possibile, impostare una password per accedere al BIOS e disabilitare nel BIOS il boot da CD/DVD o da USB
- installare solo versioni supportate e stabili evitando di installare versioni obsolete o versioni in fase di sviluppo
- installare il sistema operativo in maniera minimale
- rivolgersi ai referenti informatici della propria struttura per indicazioni sul corretto collegamento alla rete
- rimuovere i pacchetti software non utilizzati e disattivare i servizi non necessari
- assegnare una password robusta per le credenziali amministrative, cambiarla frequentemente e non riutilizzarla a breve distanza di tempo
- creare utenti locali con username nominali e non generiche, ogni utenza deve essere riconducibile ad una persona
- se la postazione è utilizzata da più utenti, ove possibile, non creare utenti locali ma abilitare l'accesso tramite i sistemi di Single Sign On di UniMORE (per es. LDAP, Active Directory, Shibboleth, ecc.)
- configurare opportunamente il firewall per impedire, limitare e monitorare l'accesso a specifiche porte o servizi
- abilitare solo le condivisioni in rete necessarie all'attività lavorativa e protette mediante l'utilizzo di credenziali di accesso
- trasferire file solo in modo cifrato (SCP, SFTP, FTPS, Rsync Over SSH)
- consentire l'accesso in remoto solo alle utenze che ne hanno la necessità e solo via RDP (Remote Desktop Connection) o SSH
- disattivare il servizio IPv6 se non esplicitamente richiesto
- installare un antivirus/antimalware e prevedere scansioni periodiche
- attivare un sistema di alert in caso di anomalie del sistema
- al termine della configurazione eseguire un backup completo del sistema per ripristinarlo in caso di compromissioni e mantenerlo offline
- aggiornare costantemente il sistema operativo con le patch di sicurezza che si rendono disponibili
- limitare i privilegi di amministratore ai soli utenti che hanno le competenze e la necessità di modificare la configurazione dei sistemi
- mantenere l'inventario delle utenze amministrative

- limitare al solo proprietario l’accesso ai file che contengono dati con particolari requisiti di riservatezza o informazioni critiche come certificati personali, chiavi private etc
- in caso di compromissioni del sistema informare immediatamente i referenti informatici della struttura
- verificare con i referenti informatici di struttura se è disponibile un log server locale o centralizzato su cui mantenere copia dei messaggi di log

RACCOMANDAZIONI DI SICUREZZA PER STAMPANTI

- Modificare subito la password predefinita dall'interfaccia web di configurazione della stampante e le community string di SNMP (solo se usato)
- Comunicare l'indirizzo della stampante a supporto.rete@unimore.it, per l'inclusione nella lista degli indirizzi il cui accesso è filtrato dal firewall di bordo
- Configurare le Access Control List (ACL) della stampante per limitare l'accesso alle subnet o ai dispositivi autorizzati
- Utilizzare connessioni crittografate quando si accede all'interfaccia web di configurazione della stampante (HTTPS, SSH)
- Disabilitare servizi/protocolli non necessari (Telnet, HTTP, FTP, SNMP, …)
- Aggiornare il firmware delle stampanti alle versioni più recenti e alle ultime patch di sicurezza

Esempi di possibili protocolli da disabilitare:

- **IPv6**, da disabilitare, la rete di Ateneo si basa su IPv4
- **Bonjour**, da disabilitare, si tratta dell'implementazione di Apple del protocollo Zeroconf di IETF e si preferisce non utilizzarlo per evitare traffico non necessario sulle reti locali
- **Porta 9100** (o HP JetDirect, socket): la maggior parte dei servizi di stampa utilizza questo protocollo, in particolare i driver di HP, quindi potrebbe non essere possibile disabilitarlo.
- **LPD**: LPD è utilizzato per la stampa da molti sistemi Unix e Linux. Tuttavia, molti possono ora utilizzare anche CUPS (Common UNIX Printing System), che consente la stampa tramite diversi protocolli. Se non si ha bisogno di LPD, occorre disabilitarlo.
- **IPP**: se il protocollo Internet Printing Protocol non è utilizzato nel proprio ambiente, disattivarlo.
- **FTP**: alcune stampanti consentono di caricare documenti FTP per la stampa. Questa funzione non è utilizzata nella maggior parte degli ambienti e dovrebbe essere disabilitata.
- **SMB**: la stampa SMB (Windows) spesso non è necessaria, poiché è gestita da altri protocolli, come JetDirect. Inoltre non è crittografata. Se possibile, disabilitare la stampa SMB.
- **SMTP**: viene utilizzato per la scansione e l'invio di fax e può essere disabilitato se non richiesto. Se necessario occorre configurarlo in modo sicuro:
    - richiedendo all'indirizzo supporto.posta@unimore.it l'abilitazione dell'IP alla spedizione mediante il server di Google
    - configurando la spedizione mediante smarthost **smtp-relay.gmail.com** , senza autenticazione, utilizzando le porte 25, 587 o 465 con SSL abilitato

- **SNMP**; da disabilitare, a meno che non sia necessario il monitoraggio della stampante tramite questo protocollo: in tal caso, occorre utilizzare delle community string diverse da quelle di default (per SNMP v1/v2) o, meglio, utilizzare SNMP v3 con credenziali utente/password che rispecchino i criteri di sicurezza generali sulle credenziali utente