Università degli Studi di Palermo

Area Sistemi Informativi
E Portale di Ateneo

Al Personale Docente e TAB

Oggetto: nuove disposizioni di sicurezza per l'accesso alla rete cablata

La sicurezza informatica è un tema particolarmente sensibile ed attuale non solo per quanto attiene la sfera privata di ciascun cittadino ma anche e soprattutto per la Pubblica Amministrazione, la quale è chiamata ad erogare un numero via via crescente di servizi digitali nel modo più sicuro possibile.
La sicurezza delle infrastrutture digitali e la riservatezza delle informazioni da queste amministrate sono state, ultimamente ancora più che in passato, messe fortemente alla prova da un numero crescente e sempre più pervasivo di attacchi informatici, accresciuti anche dalle frizioni geopolitiche che interessano Paesi a noi vicini.
In esito a tale scenario di contesto, molte infrastrutture strategiche dei Paesi occidentali in genere e del nostro in particolare sono state e, in alcuni casi, lo sono tutt'ora oggetto di cyberattacchi: il caso del cyberattacco condotto il 2 giugno u.s. al Comune di Palermo, con blocco di buona parte delle infrastrutture digitali e dei servizi erogati ed esfiltrazione di una mole assolutamente consistente di dati di cittadini ed imprese ha interessato la cronaca locale e nazionale per diversi giorni. Più di recente eventi analoghi hanno riguardato l'Università di Pisa e la Regione Sardegna.
Se da un lato non è possibile scongiurare del tutto il rischio che attacchi informatici vadano a segno con blocco delle infrastrutture ed esfiltrazione di dati sensibili, dall'altro sia il privato sia la Pubblica Amministrazione sono chiamati a porre in essere tutte le misure atte a mitigare tali rischi.
A tale riguardo, l'Università di Palermo, in conformità con il proprio vigente "*Regolamento sull'utilizzo della Rete di Ateneo e dei Servizi Internet*" emanato con D.R. n. 428/2020, con le misure minime di sicurezza AGID, con le raccomandazioni dell'ENISA (European Union Agency for Network and Information Security) e dell'Agenzia della Cybersicurezza Nazionale, intende rafforzare le misure di sicurezza informatica in vigore con nuove misure di seguito o stimolare l'adozione di buone pratiche di seguito indicate:

- attivare l'autenticazione a più fattori (MFA) per i sistemi che risultano già predisposti al suo utilizzo, quali Microsoft Office 365 e G Suite (attivazione dal 1° ottobre 2022);
- aggiornare costantemente all'ultima patch i software applicativi e di sistema;
- non utilizzare sistemi operativi non più supportati (https://docs.microsoft.com/it-it/lifecycle/faq/windows);
- effettuare il backup periodico dei dati utilizzando un sistema esterno all'unità su cui risiedono i dati stessi (esempio nel cloud di Ateneo);
- salvare i documenti di ufficio su cloud di Ateneo;
- modificare periodicamente le credenziali di accesso, utilizzando password complesse non riconducibili a fatti personali (date di nascita, nomi, indirizzi, ecc.)
- mantenere un aggiornamento costante sui temi relativi alla cybersecurity;
- rafforzare le difese dagli attacchi di tipo phishing (comunicazione inviata allo scopo di attirare una vittima):

Viale delle Scienze Ed. 11 – 90128 Palermo
segreteria.sia@unipa.it - pec: areasia@cert.unipa.it
http://www.unipa.it

- controllare sempre il link e il mittente della mail prima di cliccare qualunque indirizzo;
- prima di cliccare su un qualunque link, verificare che l'indirizzo mostrato sia davvero lo stesso indirizzo Internet al quale il link condurrà. Un controllo che può essere effettuato in modo semplice, passando il mouse sopra il link stesso;
- non condividere mai i propri dati sensibili con una terza parte. L'Ateneo e altri enti non chiedono mai informazioni del genere via email;

comunicare immediatamente al SIA eventuali incidenti o possibili situazioni a rischio (servizi non conformi, postazioni vulnerabili, ecc.). A tal proposito, a breve sarà rilasciato un servizio per le segnalazioni, nelle more usare la seguente mail: supportosia@unipa.it

Parte delle indicazioni sopra riportate vanno intese come indicazioni volte a ridurre i rischi derivanti da cyber attacchi, da effettuare direttamente a cura dell'utente, con il supporto del proprio amministratore di sistema o del SIA.
A queste indicazioni si affiancano, viceversa, una serie di interventi che il SIA si appresta a realizzare nei prossimi giorni per accrescere i livelli di sicurezza interna attraverso le seguenti azioni:

limitare l'accesso alla rete cablata solo alle postazioni autenticate tramite Global Protect, secondo il calendario in allegato; eventuali apparati presenti sulla rete di Ateneo che non possono utilizzare, per motivi tecnici, il client VPN, devono essere comunicati al SIA tramite il seguente form: https://tiny.unipa.it/apparati;

- limitare l'accesso a procedure orientate ad utenti interni all'Ateneo (protocollo, irisweb, backoffice, ecc.) solo dalla rete di Ateneo;
- disattivare tutti i servizi non a norma e migrazione degli stessi su piattaforme compatibili con i requisiti di sicurezza;
- disattivare le VPN precedenti (Openvpn, vpn.unipa.it);
- sospendere tutte le utenze di personale in quiescenza, da attivare su richiesta e su dominio diverso, come da linee guida.

Le iniziative sopra menzionate saranno realizzate nel corso delle prossime settimane, sebbene da sole non siano sufficienti a proteggerci dai rischi derivanti da cyber attacchi; tali rischi possono essere ridotti solamente tramite un uso consapevole ed attento delle risorse informatiche. Per perseguire questo obiettivo sarà necessaria la partecipazione di tutta la Comunità accademica che potrà contribuire attivamente a individuare possibili situazioni di rischio, mantenendo sempre un livello di attenzione alto durante lo svolgimento delle attività istituzionali.

Cordiali saluti.

Il Dirigente dell'Area
Dott. Riccardo Uccello
Firmato digitalmente da: Riccardo Uccello
Data: 07/07/2022 11:06:23

Il Direttore Generale
Dott. Antonio Romeo
Firmato digitalmente da: Antonio Romeo
Organizzazione: UNIVERSITA' DEGLI STUDI DI PALERMO/80023730825
Unità organizzativa: DIRETTORE GENERALE
Data: 08/07/2022 14:45:47

Il Rettore
Prof. Massimo Midiri
Firmato digitalmente da: Massimo Midiri
Organizzazione: UNIVERSITA' DEGLI STUDI DI PALERMO/80023730825
Data: 08/07/2022 17:57:39

Allegato – calendario attivazione accesso alla rete tramite VPN

A partire dalla data indicata nella tabella di seguito riportata, le postazioni presenti nel dipartimento o nell'edificio specificato, in mancanza di autenticazione VPN, non potranno più accedere alla rete internet.
Gli utenti dovranno installare prima della data indicata il client Global Protect (https://www.unipa.it/amministrazione/areasistemiinformativieportalediateneo/servizi/vpn/), eventualmente avvalendosi del supporto degli amministratori di sistema.

Data	Edificio/dipartimento
25 luglio	edificio 12
30 luglio	edificio 15 Culture e Società
5 agosto	edificio 15 Scienze Psicologiche, Pedagogiche, dell'Esercizio Fisico e della Formazione
10 agosto	edificio 3 Segreterie studenti
22 agosto	edificio 19
27 agosto	Complesso Steri
31 agosto	Aule nuove più tutto il resto dell'AOUP
10 settembre	Complesso Archirafi
15 settembre	Complesso Giurisprudenza e Scienze Politiche
19 settembre	Complesso Tukory e Agraria
26 settembre	Ed.16-18
30 settembre	Altri edifici del Campus di Viale delle Scienze e dei poli decentrati