

Le Normative

La sicurezza Digitale

Docente: Piero Bernardi

Mail e/o rif. bernardipiero@libero.it



ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI TREVISO



Associazione Ingegneri
della Provincia di Treviso

Considerazioni

- La figura dell'Ingegnere e' da sempre il tramite fra le REGOLE e le REALIZZAZIONI in tutti i campi.
- Per questo una sintesi delle NORME EUROPEE e NAZIONALI rappresenta un punto fermo da cui partire per le indicazioni che riportiamo nel seguito.



La Normativa Europea- Nazionale

EUROPA		ITALIA			
TITOLO	DATA	TITOLO	DATA	Note	Link
EIDAS – Regolamento UE 910/2014 - Electronic IDentification Authentication and Signature	23.07.2014 efficace da 01.07.2016 obbligatorio da 29.09.2018	CAD - Codice Amministrazione Digitale D.Lgs. 82/2005 – Firme Digitali – ID Elettronica – Marche Temporalì – PEC – SPID - CIE – Servizi Fiduciari.		Firme Digitali – ID Elettronica – Marche Temporalì – PEC – SPID - CIE – Servizi Fiduciari.	https://www.eid.gov.it/?lang=it https://www.agid.gov.it/it/piattaforme/eidas
Direttiva NIS – EU 2118/2016 - (Network and Information Security) EU Member states have to supervise the cybersecurity of critical market operators in their country)	2016	D.P.C.M. 17.02.2017 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali.) - D.Lgs 18.05.2018 (Attuazione NIS) – D.P.C.M. 08.08.2019 Attivazione CSIRT (Computer Security Incident Response Team)	06.05.2020	<i>La direttiva individua sette settori strategici che sono strettamente legati alla dimensione della sicurezza, ossia energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali, oltre a motori di ricerca, cloud e piattaforme online.</i>	https://www.enisa.europa.eu/ https://csirt.gov.it/ https://cert-agid.gov.it/ https://www.commissariatodips.it/
Direttiva 680/2016 – EU 689/2016	05.05.2016 efficace da 06.05.2018	D.Lgs. 51/2018	18.05.2018	<i>Trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali</i>	
RGDP – EU 679/2016 – Regolamento Generale sulla Protezione dei dati.	24.05.2016 efficace da 25.08.2018	L. 196/2003 modificata da D.Lgs. 101/2018	18.08.2018	Regolamento Europeo in materia di Protezione Dati Personali. Art 32 SICUREZZA DEL TRATTAMENTO	https://www.garanteprivacy.it/home



I riferimenti operativi

• I link di riferimenti proposti nella schermata sono utili per avere una informazione costantemente aggiornata e per chiedere o avere aiuto, in particolare:

– <https://csirt.gov.it/segnalazione> e' predisposta per segnalare attacchi ricevuti

– <https://csirt.gov.it> offre indicazioni utili per proteggersi da attacchi

– <https://cert-agid.gov.it> offre indicazioni di protezione

– <https://cert-agid.gov.it/verifica-https-cms/> link di verifica

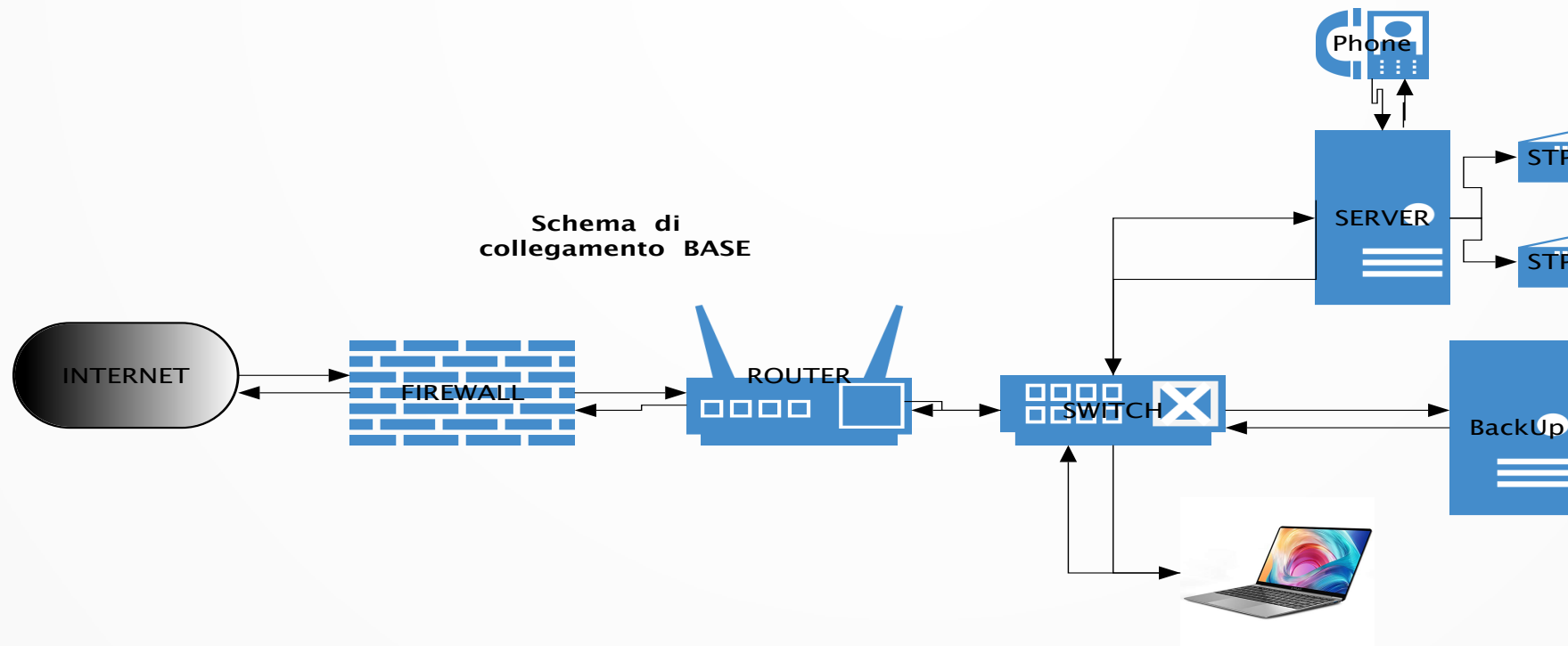
– <https://denunceviaweb.poliziadistato.it> Denuncia Reati Telematici

– <https://servizi.gpdp.it/databreach/s/> Denuncia data Breach

– <https://servizi.gpdp.it/comunicazionerpd/s/> Comunicazione RDP-DPO



Lo scopo delle nostre attenzioni



I PUNTI DEBOLI

- Le protezioni **TECNICHE** (HW – SW)
 - FIREWALL – ROUTER
 - ANTIVIRUS – ANTI-MALWARE – AGGIORNAMENTO S.O./SW
- La preparazione dell'**UTENTE**
 - Conoscenza delle forme di attacco
- La **DIMENSIONE della RETE / ORGANIZZAZIONE**
 - Disponibilità (o meno) di SERVIZIO di ASSISTENZA



IL PUNTO CRITICO

- **In una rete il punto più critico e' dato dall'UTENTE**
- Infatti i più gravi attacchi sono stati generati da azioni non corrette di utenti indotti da due fattori:
 - La **SPERANZA** (ad esempio una VINCITA ...)
 - La **PAURA** (ad esempio una CITAZIONE LEGALE ...)
- In entrambi i casi con **DECISIONI** da prendere **IMMEDIATAMENTE** sollecitate di solito al **TERMINE** di un **PERIODO LAVORATIVO** (VENERDÌ prima di un ponte festivo)



Le precauzioni da osservare

- 1 – AGGIORNARE TUTTI I DISPOSITIVI alle versioni UFFICIALI di RILASCIO del SOFTWARE.
 - Su MAC – Preferenze di sistema - Aggiornamento SOFTWARE
 - Su Microsoft – Impostazioni – Aggiornamento e sicurezza
- 2 – CONTROLLARE sempre l'aggiornamento e funzionalità ANTIVIRUS – ANTI-MALWARE
- 3 – ATTIVARE LA POLITICA DI AGGIORNAMENTO AUTOMATICO DEL FIREWALL e CONTROLLARE PERIODICAMENTE LA FUNZIONALITÀ.



Per l'UTENTE

- Utilizzare la POSTA impostando l'applicazione che gestisce la stessa affinché NON APRA le MAIL ma esponga solo il mittente e l'oggetto, chiudere la finestra di anteprima (si sono verificati casi di attacco dati dalla semplice apertura di immagini/testi).
- Modificare regolarmente la Password di accesso agli apparati/servizi avendo cura di NON utilizzare i sistemi di riproposizione automatica della Password proprie dei BROWSER.
- Controllare costantemente la buona funzionalità dell'ANTIVIRUS / ANTI-MALWARE dell'apparato.
- Se nel dubbio chiedere aiuto all'assistenza se disponibile.



Suggerimenti pratici

- La PASSWORD deve essere:
 - Composta da almeno 14 caratteri (lettere MAIUSCOLE/minuscole, numeri, segni speciali)
 - Senza senso compiuto o comunque riferibile all'utente
 - Mai condivisa con altri, ne comunicata in qualsiasi forma
- Piattaforme di verifica circa la robustezza delle password:
 - <https://www.passwordmonster.com>
 - <https://password.kaspersky.com/it/>



Una analogia

Per conquistare una fortezza sono possibili due strade

– L'attacco FRONTALE



– L'Inganno (Volontario o Accidentale) dall'interno



Esempi di Messaggi Trappola

- Riporto un esempio molto indicativo:



- Si tratta di un SMS che riporta l'esatto indirizzo associato al Cel. Per una spedizione mai avvenuta.

Bisogna fare attenzione agli SMS

- Accade che si ricevano SMS “STRANI” che chiedono di attivare collegamenti....
- **NON ATTIVATE MAI QUANTO RICHIESTO**
- Ricordiamoci che il cellulare spesso e' connesso via **WiFi** alla rete ove noi operiamo e i collegamenti che possono essere instaurati possono pregiudicare oltre che il cellulare anche le difese della rete.

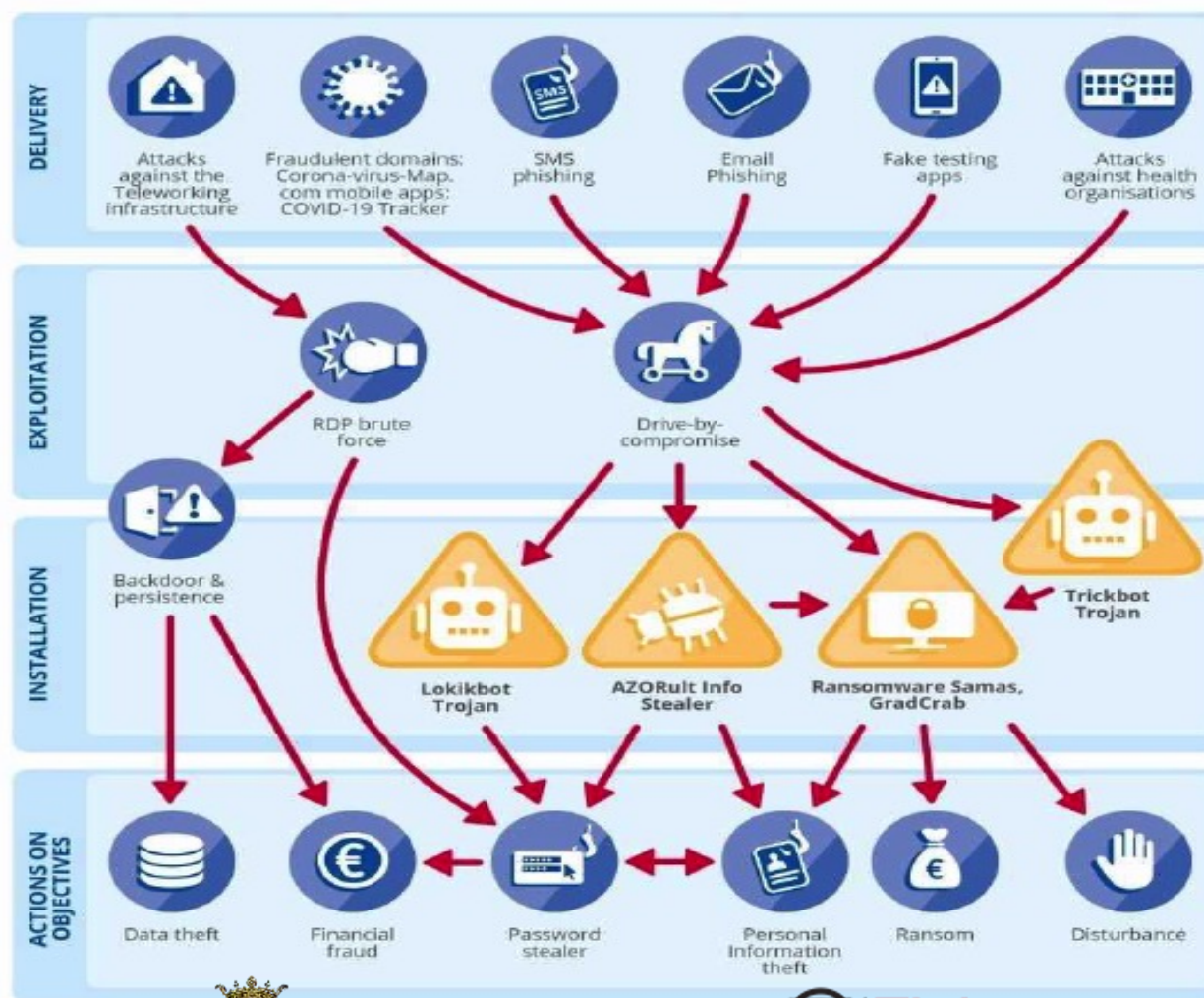


Gli attacchi digitali sotto COVID



THREAT LANDSCAPE MAPPING

Exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus (COVID-19) global pandemic.



Modalità Attacco

Modalità di Ingresso

Modalità Registrazione

Danno prodotto



ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TREVISO



I tipi di attacco registrati nel 2021

Figure 1: ENISA Threat Landscape 2021 - Prime threats



Tipologie di attacco

Ransomware	Blocco con crittografia dati organizzazione con richiesta riscatto
Malware	Sw che opera sia su base Sw sia Hw eseguendo processi che impattano riservatezza e integrità del sistema
Criptojackking	O cripto mininig uso delle risorse del sistema per acquisire cripto valute
Minacce su posta elettronica	Vengono attuate sulla base della dabbenaggine degli utenti e veicolano spesso Sw portatori di svariate tipologie di attacco.
Minacce contro i dati	Questo può avvenire sia per violazione sia per fuga di dati/informazioni a causa di attacco o perdita anche involontaria dei dati. (in genere sfociano in estorsioni ..)
Minacce alla disponibilità e integrità	In genere sono legati a tipologie quali attacchi Denial of Service (DoS) e/o Web Attacks. Sono attacchi che tendono ad esaurire le risorse del sistema causando perdita di dati ed interruzione del servizio
Disinformazione	E' una nuova tipologia di attacco e si sviluppa per ridurre la percezione di fiducia e attenzione per favorire forme diverse di attacco.
Minacce non dannose	In sostanza errori umani o malfunzionamenti/disastri fisici che portano comunque perdita di dati.



Esempi di messaggi pericolosi

- Messaggi veicolati per posta elettronica del tipo
- Devono indurre il destinatario a procedere
- Alla verifica del mittente nel caso:
- info@tibumedia.net tramite una ricerca su
- Sistemi che riportano l'attendibilità del mittente



La verifica del mittente

• Quando arrivano messaggi non attesi con caratteristiche sospette la cosa migliore e' quella di controllare, tramite servizi disponibili in rete, l'attendibilità del mittente, ad esempio usando:

<https://mxtoolbox.com/blacklists.aspx>



La verifica

• Utilizzando il servizio **MxToolBox** si ottiene:

The screenshot shows the MxToolBox SuperTool interface. The main content area displays the results of a blacklist check for the domain **tbumedia.net**. A prominent message states: "BLACKLISTING isn't the ONLY email delivery issue". Below this, a notification indicates: "We notice you are on a blacklist. Click here for some suggestions".

The results section shows the following data:

	Blacklist	Reason	TTL	ResponseTime	
✗ LISTED	UCEPROTECTL2	160.153.129.219 was listed	2100	1	Ignore
✗ LISTED	UCEPROTECTL3	160.153.129.219 was listed	2100	2	Ignore
✓ OK	ivmURI			1	
✓ OK	Nordspam DBL			3	
✓ OK	SEM FRESH			35	
✓ OK	SEM URI			35	
✓ OK	SEM URIRED			35	
✓ OK	SEDRSUSLBARCONE			0	



Un utile strumento – Misure Minime di Sicurezza

- La Circolare AgID n. 2 del 18.04.2017 riassume i punti fondamentali che possono garantire la sicurezza della rete.
- La circolare è un elemento di riferimento obbligatorio per le Pubbliche Amministrazioni ma rappresenta un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle organizzazioni (almeno quelle di una certa importanza).
- Il Link: <https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict>



Una misura semplice ma spesso trascurata

- Per qualsiasi organizzazione, dalla multinazionale allo studio personale, la copia di **BACKUP** è l'elemento **BASILARE** per garantire la sicurezza sia da attacchi (RANSOMWARE) sia da malfunzionamenti sempre possibili degli apparati.
- Riporto i metodi che consentono il salvataggio delle macchine in ambiente Mac (Time machine) o in ambiente Windows 10 (Aggiornamento e sicurezza), sempre che si disponga di un disco esterno connesso in modalità USB alla macchina:

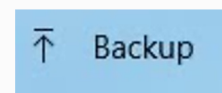
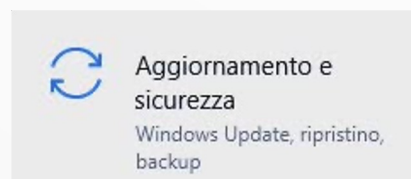


il BACKUP

- Per Mac da “Preferenze di sistema”












- Per Windows da “Impostazioni”



A che serve un FIREWALL

- Un FIREWALL ben organizzato consente di EVIDENZIARE gli IP di coloro che cercano di entrare nella rete, riportandoli in appositi registri.

Tipo	Data	Ora	Server	Utente	IP sorg...	Nome c...	Contenuto
	2021/08...	21:37:59	NAS2TBT	System	127.0.0.1	localhost	[Network & Virtual Switch] Stopped Network & Virtual Switch.
	2021/08...	21:37:38	NAS2TBT	System	127.0.0.1	localhost	[App Center] Stopped Media Streaming Add-on.
	2021/08...	21:36:04	NAS2TBT	admin	192.168...	--	[Power] Restarting NAS.
	2021/08...	21:36:02	NAS2TBT	System	127.0.0.1	--	[Security] Removed IP "213.152.186.168" from IP block list.
	2021/08...	21:30:53	NAS2TBT	admin	213.152...	--	[Users] Failed to log in via user account "admin". Source IP address: 2...
	2021/08...	21:30:52	NAS2TBT	System	127.0.0.1	--	[Security] Added IP address "213.152.186.168" to IP block list. Duratio...
	2021/08...	21:30:51	NAS2TBT	admin	213.152...	--	[Users] Failed to log in via user account "admin". Source IP address: 2...
	2021/08...	21:30:48	NAS2TBT	admin	213.152...	--	[Users] Failed to log in via user account "admin". Source IP address: 2...
	2021/08...	21:30:46	NAS2TBT	admin	213.152...	--	[Users] Failed to log in via user account "admin". Source IP address: 2...

- in modo da bloccare, tramite specifiche funzioni, gli IP dannosi.

Due utili servizi

- Per conoscere se un IP è stato VIOLATO e fonte di PERICOLO:
 - <https://www.abuseipdb.com/>
 - <https://www.abuseipdb.com/categories>
- Per conoscere la reputazione del proprio IP e quindi comprendere se si è stati compromessi:
 - https://talosintelligence.com/reputation_center
- Entrambi i siti sono ricchi di riferimenti e documentazione.



La sicurezza e' ..

- E' una questione vitale al giorno d'oggi tenuto conto del fatto che esiste un **MERCATO** dei **DATI PERSONALI**, oltre che degli **ACCESSI** (Utenti e Password), che rende appetibile ai malfattori digitali quasi ogni tipo di connessione...
- L'utente è la parte più facilmente attaccabile: è sempre necessario che un tecnico (esperto) abbia proceduto ad un corretto dimensionamento delle protezioni della rete e istruito l'utente all'utilizzo sicuro degli apparati.



Le Chiavette USB

Le chiavette USB rappresentano un sistema
Comodo ed efficiente per condividere file
Anche di grandi dimensioni.

ATTENZIONE

Solo con apparati configurati in modo tale da
CONTROLLARE all'accesso lo stato virale dei
Supporti è ragionevole utilizzarle.



Grazie per l'Attenzione



ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI TREVISO



Associazione Ingegneri
della Provincia di Treviso