Il percorso verso MMS-PA e GDPR

- Situazione sulla sicurezza ICT
- Modello Organizzativo adottato
- Azioni effettuate per le MMS-PA e GDPR

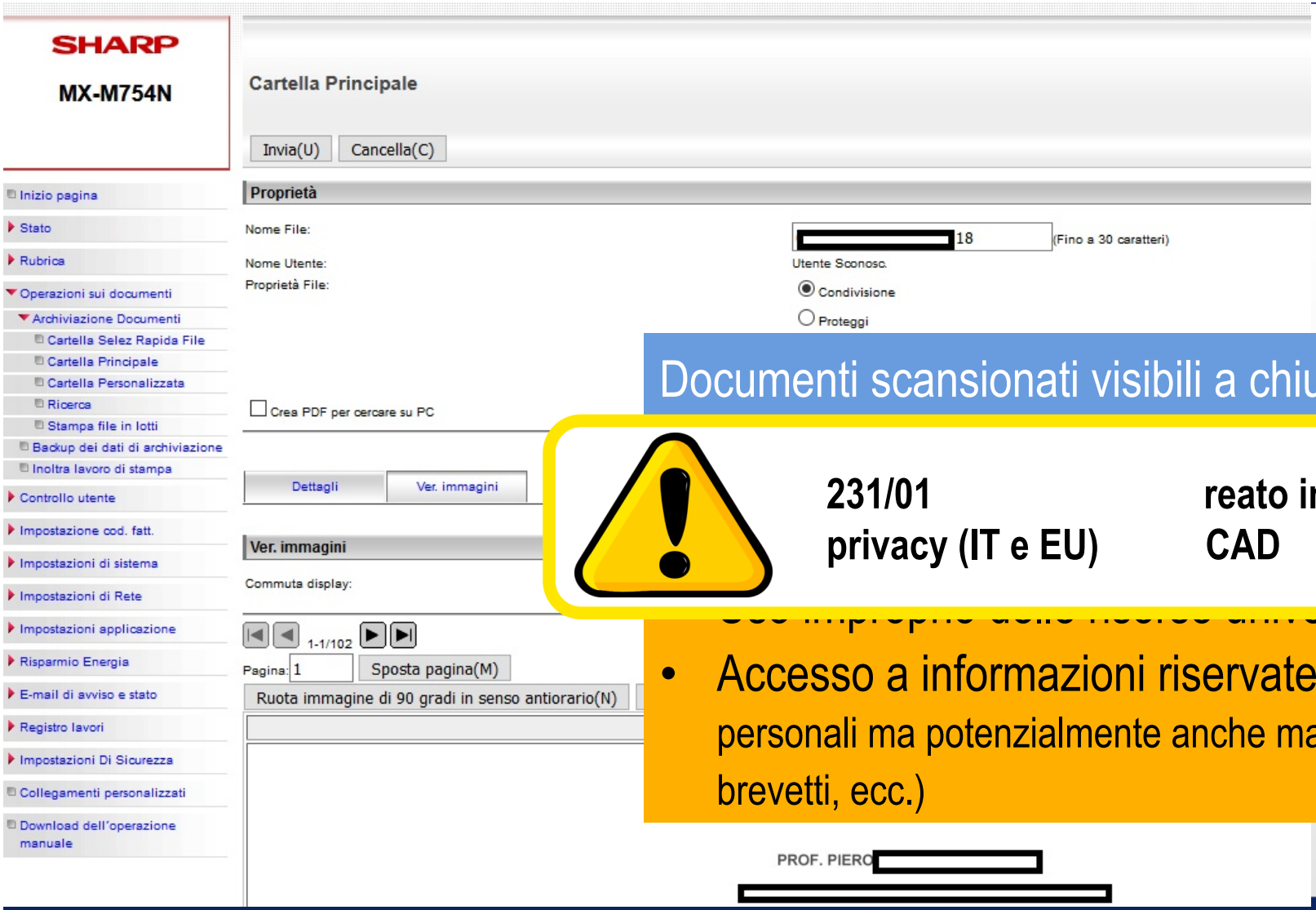
Premessa Problematiche di sicurezza ICT

- Elevato numero di nodi connessi in rete: circa 35.000 al giorno

- Nodi «visibili», raggiungibili dall'esterno con servizi attivi:
  - servizi: server, stampanti, NAS, telecamere, internet delle cose (IoT)
  - Assenza, spesso, di misure idonee sui sistemi e sui dati:
    - malconfigurazioni e vulnerabilità HW e SW sui dispositivi connessi
    - Sistemi obsoleti
    - Sistemi in rete senza soluzioni di sicurezza a bordo (antivirus, fw personali,..)

- Scarsa consapevolezza degli utenti su norme di buon comportamento:
  - uso di credenziali deboli o usate anche su altri siti,
  - uso di SW illegale o non affidabile
  - Ingenuità nell'aprire mail contenenti allegati o link malevoli
  - Accesso a siti compromessi contenenti SW malevolo.

Stampanti multifunzione accessibili



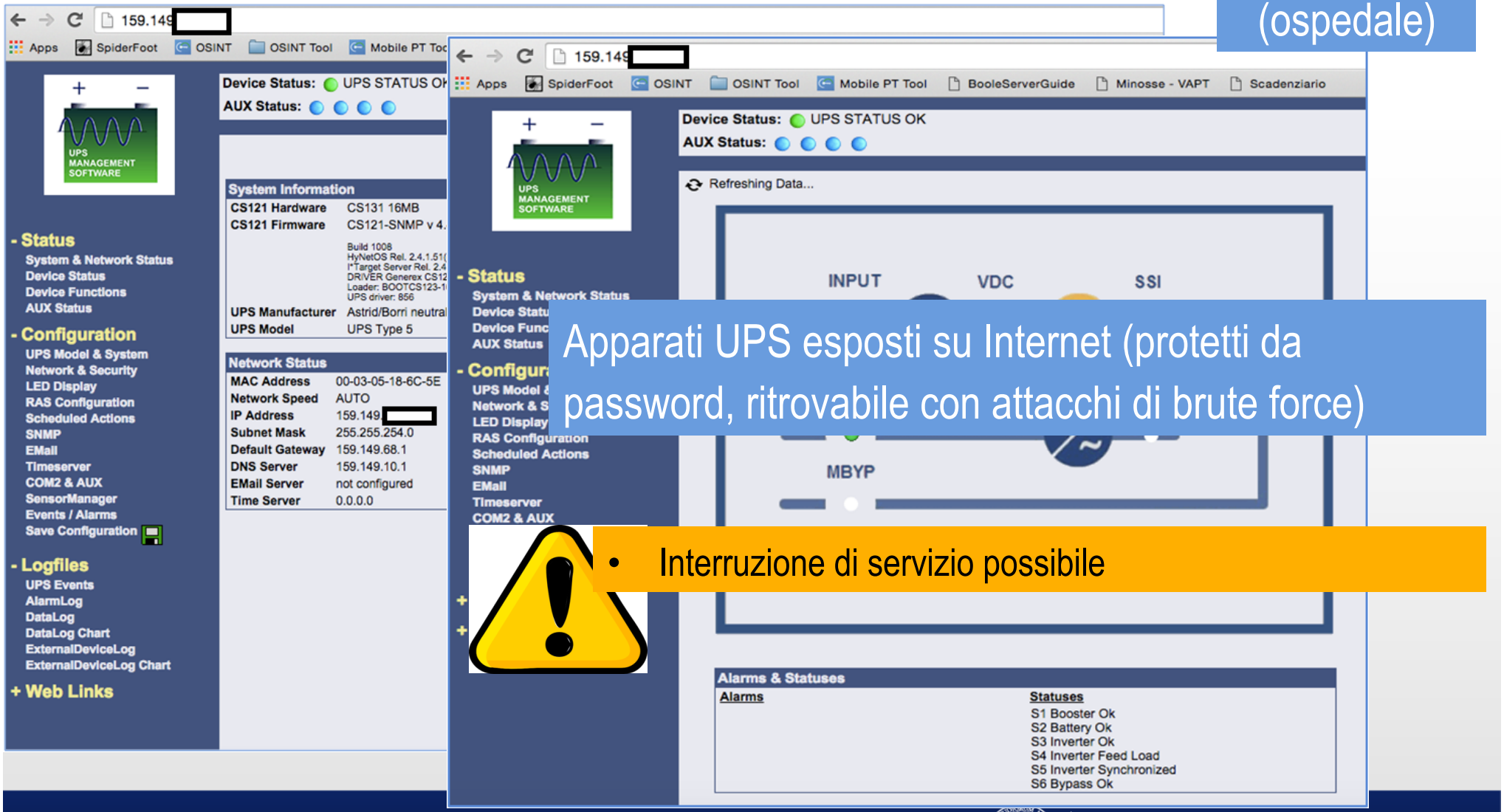
Documenti scansionati visibili a chiunque si colleghi

231/01
privacy (IT e EU)
reato informatico
CAD

- Accesso a informazioni riservate (documenti personali ma potenzialmente anche materiale di ricerca, brevetti, ecc.)

Interfacce di gestione UPS esposte

Dipartimenti (ospedale)

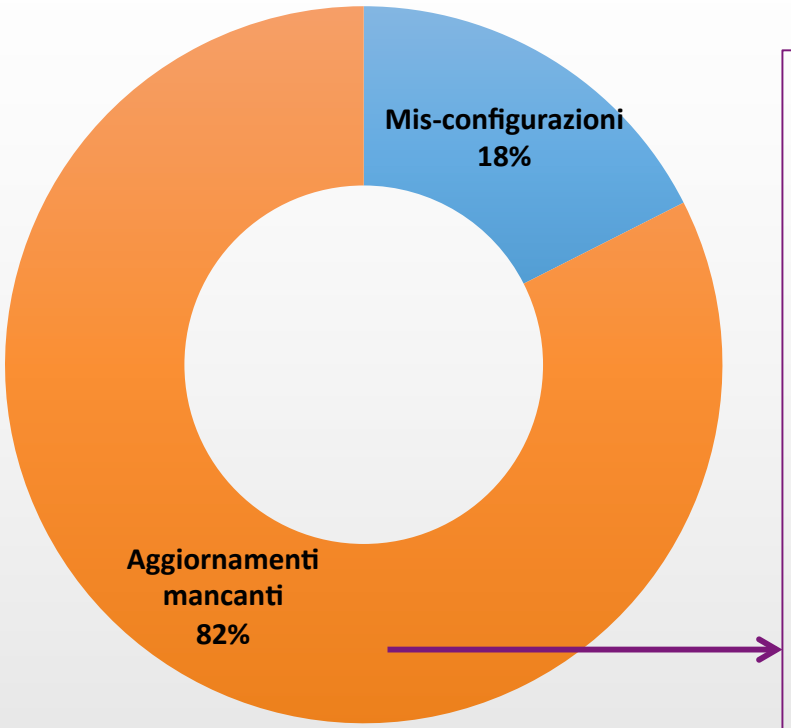


Apparati UPS esposti su Internet (protetti da password, ritrovabile con attacchi di brute force)

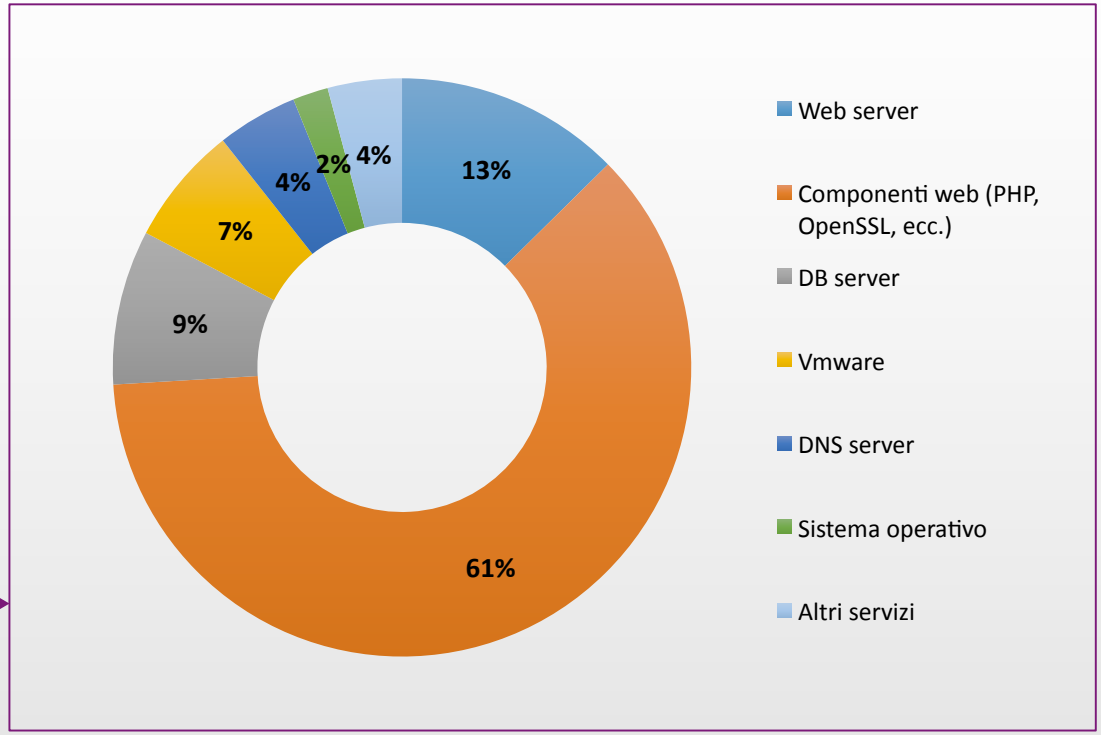
- Interruzione di servizio possibile

tipologie di problemi nei Dipartimenti

DIPARTIMENTI



Aggiornamenti mancanti per categoria di di sistema o servizio



Dati sugli interventi relativi alla sicurezza ICT

Anno	Tipo di Incidenti Sicurezza					
	compromesso	ddos compiuto da Interno	presunta pirateria	spam	Malconfiguraz. Segnalate da fonti esterne	Dispositivo non autorizzato con impatto su funzionamento rete
2016	58	4	188	14	40	9
2017	17	0	38	9	3	38

Anno	Azioni Prevenzione					
	Azioni di quarantena su nodi interni	Protezione da phishing ai danni UNIMI	Rilevazione Malconfig	Protezione Sistemi Informativi AntiDDOS	Threat FW Garr	Tentativi di Compromissione da Esterno
2016	2349	0	51	0	39.825.221	357.781
2017	2236	3	301	3	27.803.626	118.927

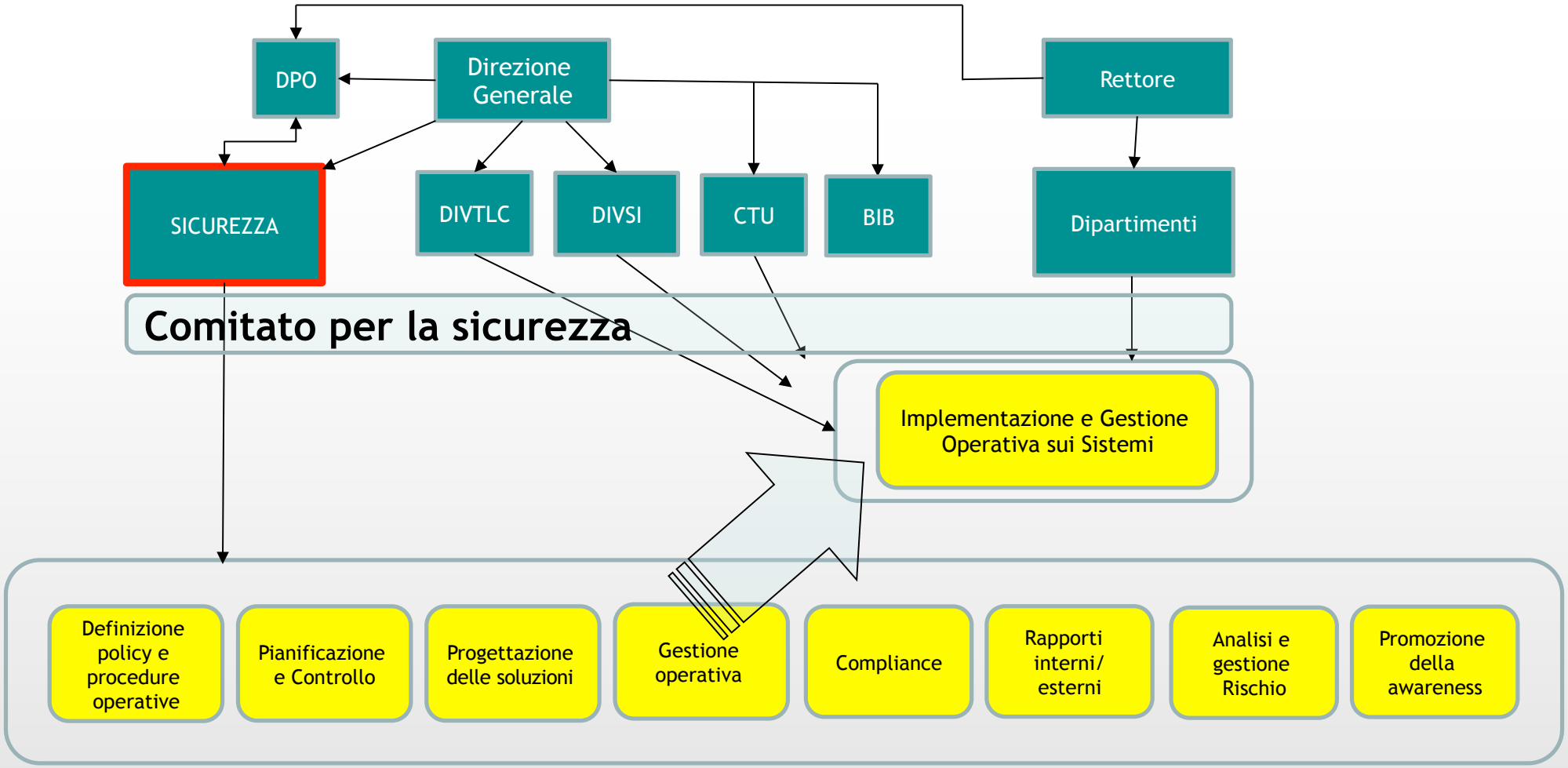
I dati non riportano i casi di violazioni di credenziali unimi che spesso causa spam da server di Ateneo

Verso un nuovo Modello

- *Deadline* stringenti in ambito Normativo:
  - Misure minime di Sicurezza per le P.A. **(31/12/2017 !!)**
  - Nuovo GDPR in materia Protezione dei dati **(24/5/2018 !!)**

- Creazione di una Nuova Struttura per la governance e la gestione dedicata alla Sicurezza ICT e alla protezione dei dati

Che fare? Una struttura unica di Governance e di Gestione della Sicurezza ICT e protezione Dati



MMS-PA: ABSC (AgID Basic Security Controls) 1/3

ABSC 1: Inventario dei dispositivi autorizzati e non autorizzati

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC 2: Inventario dei software autorizzati e non autorizzati

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

ABSC 3: Proteggere le configurazioni hardware e software sui dispositivi mobili, laptop, workstation e server

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

MMS-PA: ABSC (AgID Basic Security Controls) 2/3

ABSC 4: Valutazione e correzione continua delle vulnerabilità

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC 5: Uso appropriato dei privilegi di amministrazione

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC 8: Difese contro i malware

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

MMS-PA: ABSC (AgID Basic Security Controls) 3/3

ABSC 10: Copie di sicurezza

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

ABSC 13: Protezione dei dati

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti.

Struttura di Sicurezza ICT

È in staff alla Direzione Generale

Punto di riferimento unico TECNICO e TECNICO-LEGALE

- Si occupa di protezione dell'infrastruttura, sistemi, servizi
  - Protezione della rete e di ciò che è connesso alla rete
  - Prevenzione delle intrusioni e reazione agli attacchi
  - SOC, IRT, VA,
  - Progettazione soluzioni architetturali
  - Gestione Sicurezza ICT (10 firewall, piattaforma siem, AV, VPN)

- Si occupa di protezione dei dati, personali e strategici
  - Disponibilità
  - Confidenzialità
  - Integrità
- Procedure e azioni a tutelare i dati e la compliance

Cosa ha fatto l'Ufficio Sicurezza ICT su Misure Minime di Sicurezza per le PA: 2017

- Partecipazione a Gruppo Di Lavoro CODAU
- Riunione con Direttori e Responsabili Strutture sulle MMS-PA
- Interazione con le strutture per individuazione Referenti
- Incontri tecnici con i Referenti per compilazione
- Redazione di Documentazione e Linee Guida Operative alla compilazione delle schede:
  - Vademecum
  - Esempi di compilazione delle Schede
  - Addendum Dipartimenti
- Supporto a tutte le strutture coinvolte per chiarimenti, indicazioni, delucidazioni
- Suggerimenti su Policy interne
- Attività di Prevenzione Compromissione e incidenti di Sicurezza

MISURE MINIME SICUREZZA per le PA - Amministrazione

- Per le strutture gestite centralmente (ad es. Amministrazione Centrale) la compilazione delle Schede relative alle misure Minime è stata effettuata dalle strutture Centrali IT.

Tipologie di Risorse in Dipartimento

- Postazione Amministrative/gestionali
- Macchine Docenti e Server di ricerca (in genere Direttore via policy delega applicazione MMS a docenti)
- Server dipartimentali
- Aule, strumenti di ricerca,---

In alcuni casi Viene dichiarato di non riuscire a fare alcuni controlli o ridotto Perimetro

- Inventario: Macchine di Segreteria (Direzione, Generali, Didattiche, amministrative) e Stampanti
- Server Dipartimentali (registraz. Server)
- Altre postazioni: norme interne
- Non controllo di chi accede alla rete cablata
- Dichiarazione di controlli non effettuati

Criticità Rilevate nelle strutture periferiche - DIDATTICA E RICERCA

- Alcuni Strutture:
  - non hanno un presidio IT o talvolta senza adeguato Know how
  - Distribuite su varie sedi
  - Macchine e server di ricercatori/docenti autoamministrate
  - Macchine
    - obsolete e vulnerabili
    - malconfigurate
  - Apparati di Rete Abusivi
  - Uso risorse IT di utenti non strutturati in luoghi con accessi fisici non presidiati
  - Situazioni Complesse
    - Presenza di Personale non UNIMI: CNR
    - Ospedali
    - …

Azioni delle Strutture per le Misure Minime di Sicurezza

- Censire e aggiornare inventario
- Registrazione Risorse (server, stampanti, telecamere, NAS, sensori, ..) su DB centrale
- Installazione Antivirus di Ateneo:
- Aggiornamento sistemi e applicativi
- Gestione delle postazioni
- Applicazione delle misure opportune per la protezione dei sistemi e dei dati
- Non usare credenziali unimi su servizi esterni
- Evoluzione verso una centralizzazione dei dati/servizi?

Ricadute Positive delle MMS-PA ma è solo l'inizio

- Macchine Obsolete
  - Eliminazione di alcune
  - Identificazione
- Censimento e in alcuni casi identificazione Asset
- Policy Interne
  - Accesso alla rete di studenti, visitor professor, frequentatori, collaboratori attraverso la rete WIFI Eduroam -> VS accesso libero alla rete cablata senza controllo
  - Divieto rogue Apparati
  - Rispetto MMS-PA
- Potenziamento uso AV unimi
- Inizio del Processo di Sicurezza

Richiesta di Supporto a Servizi Centrali

- Ufficio Sicurezza
  - Vulnerability Assessment
  - Definizione del Piano di Gestione del Rischio
  - Analisi del Rischio
  - Guida nella scelta di strumenti utili alla Sicurezza: ad es. per inventario HW e/o SW [inventario manuale diventa OBSOLETO]
  - Consulenza su applicazione di misure sicurezza
  - Soluzioni AV più «leggere»

Ma anche

  - Gestione postazioni (almeno alcune tipologie)
  - Servizi di Backup
  - Servizi di Cloud Interno (alternativo a DropBox)
  - Estensione e potenziamento Eduroam

Azioni 2018 Ufficio Sicurezza

- REVISIONE POLITICHE DI SICUREZZA ATENEO
- AZIONI MIGLIORAMENTO SICUREZZA VERSO
  - STRUTTURE IT CENTRALI
  - AMMINISTRAZIONE
  - ALTRE STRUTTURE (es. Dipartimenti)
  - INDIVIDUAZIONE MACCHINE CON VULNERABILITA' O MALCONFIGURAZIONI
  - POTENZIAMENTO ATTIVITA' DI PREVENZIONE

GDPR IN UNIMI

Roadmap per il GDPR

1. Creazione Nuova Struttura Sicurezza ICT così articolato:
2. Partecipazione al GDL Codau per GDPR in ambito Universitario
3. Creazione di un COMITATO sulla Sicurezza informatica e Conformità al trattamento dati
4. Formazione GDPR obbligatoria per tutti:
    1. Formazione in AULA Dedicata a Management
    2. Referenti in AULA TECNICI
    3. Attivazione Modalità Elearning per PTA
    4. Prossimamente per componente Docente, Ric, etc..
5. Nomina del Responsabile della protezione dei dati (Data Protection Officer)
6. Questionario On line per censimento
7. Redazione del registro dei trattamenti
8. revisione dei modelli di informativa e consenso
9. creazione di una procedura per la comunicazione della violazione di dati personali
10. revisione delle policies di utilizzo degli strumenti informatici e di trattamento dei dati
11. Conduzione di una valutazione d'impatto privacy

PREMESSA

- Il GDPR impone una governance nella gestione dei dati, un ripensamento dei processi e conoscenza dei flussi dei dati
- Si basa sulla responsabilizzazione e sulla consapevolezza
- Impone cambiamenti anche nel modo di operare quotidiano

Linee Guida a cura del GdL Codau su GDPR

Unimi ha partecipato al gruppo di Lavoro Codau per la redazione delle linee guida in materia Privacy e protezione Dati in ambito universitario

Linee guida in materia di privacy e protezione dei dati personali in ambito universitario

Versione 1.1 – novembre 2017

Redazione a cura di:

Nicla Diomede (Università degli Studi di Milano – Statale)

Pasquale Ficara (Università degli Studi di Milano-Bicocca)

Alessandra Magri (Università degli Studi di Milano-Bicocca)

Marisa Morbidi (Università degli Studi di Firenze)

Fabrizio Pedranzini (Politecnico di Milano)

Daniela Prestipino (Università degli Studi di Messina)

Paolo Sanna (Università degli Studi di Milano – Statale)

Manuela Zecca (Alma Mater Studiorum – Università Bologna)

Revisione a cura del Gruppo di lavoro "Linee Guida Privacy e GDPR" del CODAU

Linee Guida GDPR in ambito Universitario

- Novità, soggetti del trattamento, Finalità istituzionali
- Mappa dei Trattamenti (studenti, personale, terzi)
- Ricerca Scientifica e Statistica -->progetti di ricerca
- Allegati:
  - approfondimento per redazione informative
  - Scheda di analisi per progetti di ricerca
  - Informativa per trattamento dati sensibili in un progetto di ricerca

Roadmap di Unimi

1. Creazione dell'Ufficio di Staff Sicurezza ICT (sicurezza.ict@unimi.it) così articolato:
   - Protezione Infrastrutture, Sistemi e Servizi (soc@unimi.it)
   - Tutela Dati (tuteladati@unimi.it)
2. Creazione di un comitato ad hoc sulla Sicurezza informatica e Conformità al trattamento dati
3. Azioni formative sul GDPR
4. Nomina di un Responsabile della protezione dei dati (Data Protection Officer)
5. Redazione di un registro dei trattamenti
6. Conduzione di una valutazione d'impatto privacy
7. revisione dei modelli di informativa e consenso in uso presso UniMi
8. revisione delle policies di utilizzo degli strumenti informatici e di trattamento dei dati personali
9. creazione di una procedura per la comunicazione della violazione di dati personali

Censimento dei trattamenti

- Scheda con richiesta informazioni per ciascun trattamento
- Indicare Società che trattano dati personali e scadenza
- Esistono Informative Specifiche?
- Persona di Riferimento privacy → anche per Seminario di Formazione

Quindi?

- Da dove partire?
- Censimento Attività di Trattamento
- Messa in sicurezza di quelli più rischiosi

CONCRETAMENTE: individuazione trattamenti più a rischio

- **INDIVIDUARE LE ATTIVITA' DI TRATTAMENTO CHE POSSONO RISULTARE MAGGIORMENTE CRITICHE PERCHE' RIGUARDANO**
  - AD ES. CATEGORIE PARTICOLARI DI DATI PERSONALI
  - NUMERO ELEVATO DI INTERESSATI
  - TRATTAMENTO DI PROFILAZIONE
- **DOVE SONO I DATI? Con Quali strumenti sono acceduti??**
  - ATENEO:
    - MACCHINE LOCALI ALLA STRUTTURA: SERVER? NAS? CHIAVETTE? PC/PORTATILI?
    - SERVIZI INFRASTRUTTURALI SERVIZI CENTRALI (ad es. Server Divsi, UnimiBox, ..)
  - DATI ESTERNI AD UNIMI:
    - ALL'ESTERO? EXTRA UE?
    - SERVIZI CLOUD esterni (DROPBOX, Google DRIVE)
    - Servizi Infrastrutturali Ministeriali (es UGOV, CINECA, loginmiur)
    - sistemi di enti/partner/aziende/ospedali;
- **Come sono scambiati? e-mail Unimi SI/no; email esterne; Protocolli Sicuri?**
- **PER QUANTO TEMPO? QUALI MISURE DI SICUREZZA?**

ES. DI CATEGORIE DI INTERESSATI in UNIMI

- - Personale docente e ricercatore
- - Personale tecnico e amministrativo
- - Studenti
- - Dottorandi
- - Lavoratori autonomi
- - Assegnisti di ricerca
- - Specializzandi
- - Collaboratori occasionali
- - Soggetti esterni (di vario tipo)
- - Minori di 16 anni (13-16 anni)
- - Altro

NATURA DEI DATI

- - Personali (comuni)
- - Origine razziale
- - Origine etnica
- - Opinioni politiche
- - Sanitari
- - Genetici
- - Biometrici
- - Campioni biologici
- - Giudiziari

Dati personali protetti dal segreto professionale
Dati di comunicazione elettronica
Dati di geolocalizzazione
Dati finanziari
Appartenenza sindacale
Convinzioni filosofiche
Convinzioni religiose
Vita sessuale, Orientamento sessuale

Individuare se all'interno della propria Struttura si trattano dati che, in generale, possono aumentare il rischio potenziale per i diritti e le libertà delle persone

Individuazione dei Trattamenti per Valutazione Impatto ai fini Privacy

- Processi valutativi automatizzati e sistematici o profilazione
- Decisioni automatizzate con conseguenze giuridiche
- Sorveglianza sistematica
- Elaborazione di dati su larga scala che ha conseguenze per un gran numero di parti interessate
- Interconnessione di raccolte di dati che le persone interessate non possono ragionevolmente prevedere
- Il trattamento dei dati implica che gli interessati non possono esercitare un diritto, non possono utilizzare un servizio o non possono stipulare un contratto
- Uso di nuove tecnologie o applicazione di mezzi tecnici e organizzativi
- Monitoraggio sistematico su larga scala di un'area accessibile al pubblico.
- Altro

Esempi di Misure di sicurezza Tecniche

- Pseudonomizzazione dei dati personali
- Cifratura dei dati personali
- Autenticazione
- Firewall
- Antivirus
- Disaster Recovery
- Backup
- Altro Specificare
- QUINDI
- custodire i dati su dispositivi Sicuri e protetti
- → **Registrare Server/NAS/dispositivi e informare Ufficio Sicurezza ICT**

Esempi Misure Organizzative di Sicurezza

- Istruzione per il trattamento
- Accesso Controllato;
- Armadi chiusi;
- Policy Aziendali
- Formazione
- Altro specificare

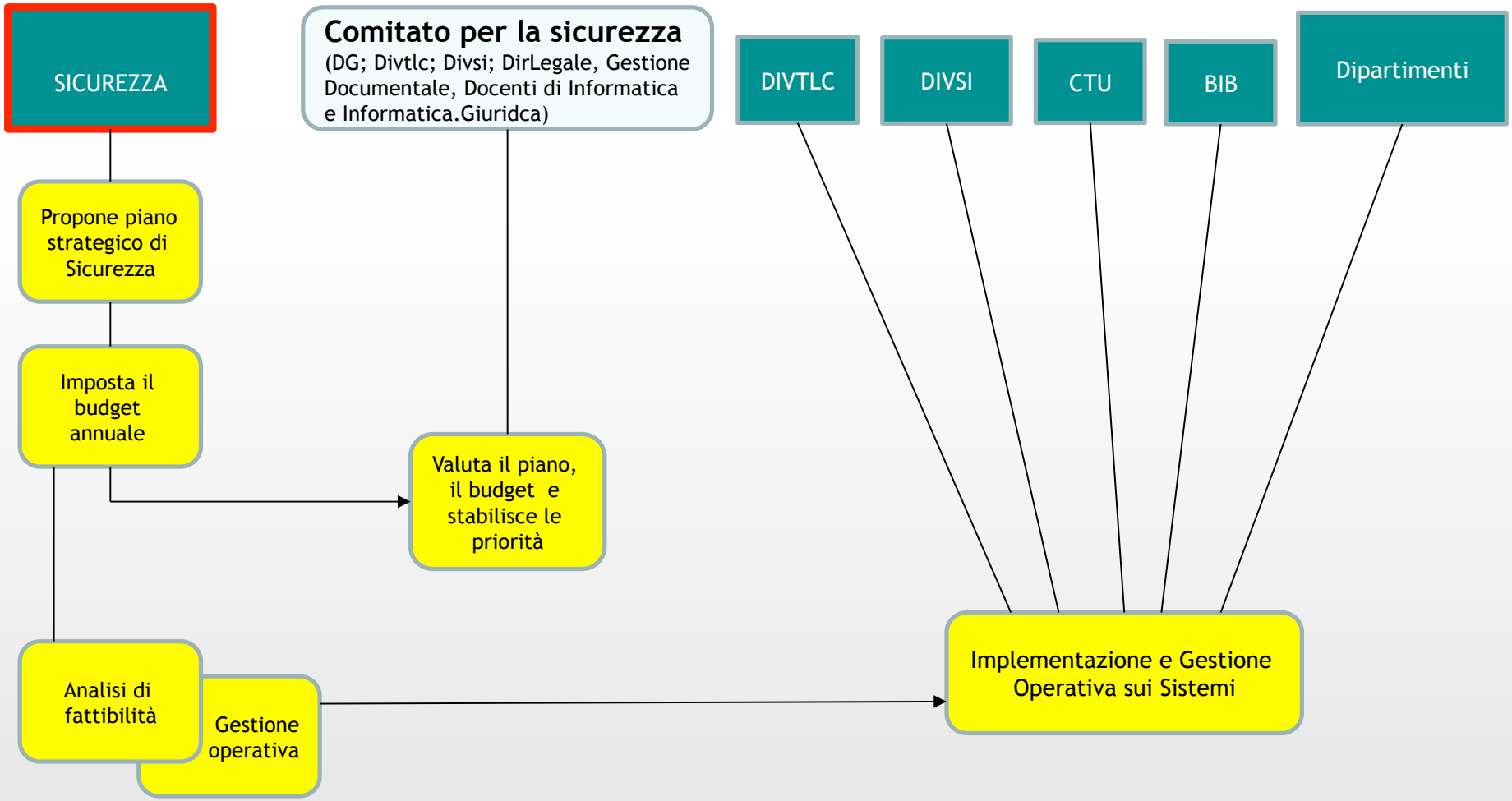
Es. Categorie di destinatari

- M.I.U.R., C.U.N.
- INPS; INAIL,
- MAE INAIL,
- Autorità di P.S. e Autorità Giudiziaria,
- Strutture sanitarie
- Istituti Bancari
- Aziende Partecipate
- Altre Università italiane e straniere
- Organizzazioni internazionali
- Soggetti pubblici e privati ai quali viene affidato il servizio di formazione del personale;
- Soggetti privati ai quali l'Ateneo affida dei servizi di propria competenza in out-sourcing;
- ATS e ASST per docenti medici con funzioni assistenziali
- Unione Europea
- Altri enti di ricerca

GRAZIE

Nicla Diomede
Sicurezza ICT di Ateneo – Direzione Generale
E-mail: nicla.diomede@unimi.it

La Sicurezza ICT nell'organizzazione Unimi



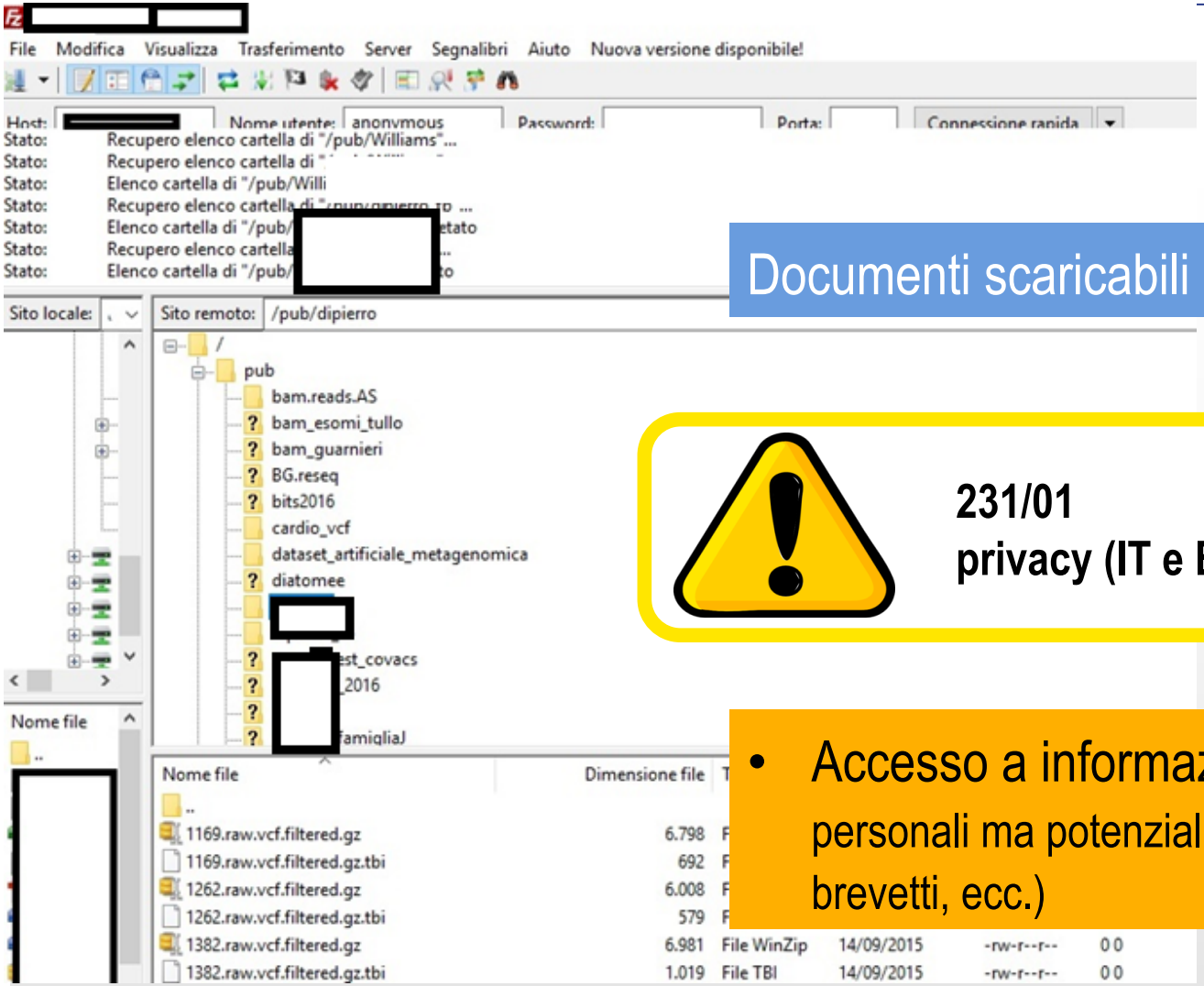
Governance e Gestione sinergica Sicurezza e Protezione Dati

- Gestione omogenea, condivisa e organizzata
- Definizioni chiare su ruoli e responsabilità
- Policy di Ateneo
- Awareness
- Procedure di Incident Management
- Partecipazione attiva ai processi di sviluppo di nuovi servizi o nuove tecnologie per la corretta e completa identificazione dei requisiti di sicurezza, la loro valutazione e il loro recepimento nelle soluzioni sviluppate («security by design»);
- Attivazione di verifiche interne periodiche complessive o puntuali sui livelli di sicurezza implementati;
- Definizione, mantenimento e attivazione di procedure, organizzazioni e soluzioni per la gestione degli incidenti di sicurezza informatica e di eventi disastrosi
- Canali ufficiali per comunicazioni e informazioni

Mission della Struttura: creazione di una regia

- Predisposizione policy di sicurezza, best practice organizzative e/o procedurali per il mantenimento dei livelli di sicurezza prefissati, soluzioni tecnologiche per l'implementazione di misure di sicurezza;
- Promozione di azioni sinergiche e coordinate tra le diverse componenti coinvolte in ambito Sicurezza
- Partecipazione attiva ai processi di sviluppo di nuovi servizi o nuove tecnologie per la corretta e completa identificazione dei requisiti di sicurezza, la loro valutazione e il loro recepimento nelle soluzioni sviluppate («security by design»);
- Attivazione di verifiche interne periodiche complessive o puntuali sui livelli di sicurezza implementati;
- Definizione, mantenimento e attivazione di procedure, organizzazioni e soluzioni per la gestione degli incidenti di sicurezza informatica e di eventi disastrosi;
- Security warning;
- Analisi e gestione del rischio informatico;
- Formazione e informazione al personale con l'obiettivo di aumentare la sensibilità e la consapevolezza del rischio cyber.

Servizi FTP con possibilità di accesso anonimo ai Dati



Dipartimenti

Documenti scaricabili da chiunque si colleghi

231/01
privacy (IT e EU)

reato informatico
CAD

- Accesso a informazioni riservate (documenti personali ma potenzialmente anche materiale di ricerca, brevetti, ecc.)

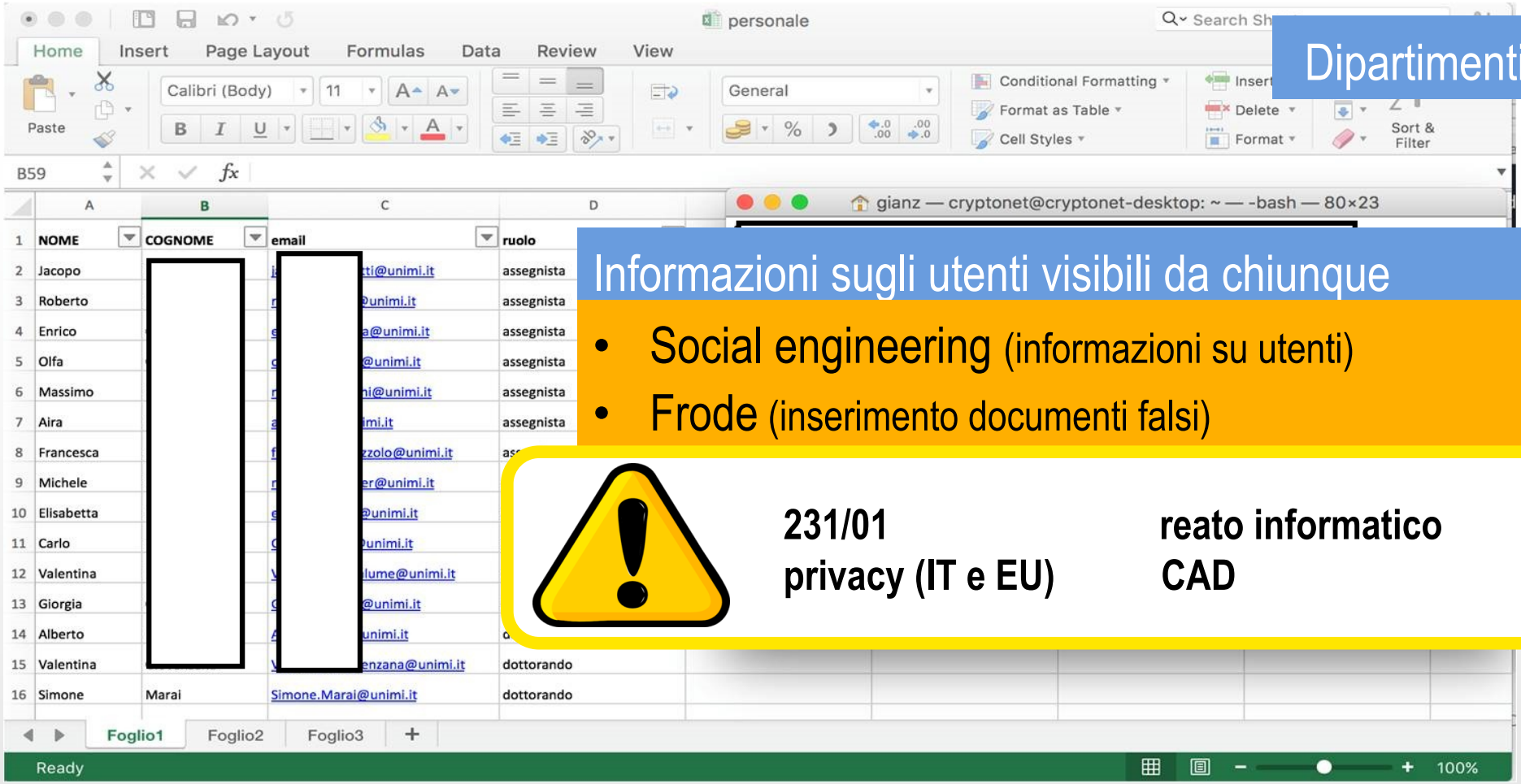
Console di management con account di default

Possibilità di vedere o alterare la configurazione

231/01 **reato informatico**

- Uso improprio delle risorse universitarie

Share accessibili pubblicamente in scrittura



Dipartimenti

Informazioni sugli utenti visibili da chiunque

- Social engineering (informazioni su utenti)
- Frode (inserimento documenti falsi)

231/01
privacy (IT e EU)

reato informatico
CAD

Access Point Wireless Autorizzati e non configurati

Dipartimenti (ospedale)

159.149.8[redacted]/wireless_wpa_psk_wpa2_psk.htm

Apps | SpiderFoot | OSINT | OSINT Tool | Mobile PT Tool | BooleServerGuide | Minosse - VAPT | Scadenzia

BELKIN. Router Setup

Wireless
Channel and SSID
Security
Guest Access
WPS
Use as Access Point
MAC Address Control
Utilities
Restart Router
Restore Factory Default
Save/Backup Settings
Restore Previous Settings
Firmware Update
System Settings

Wireless > Security

Security Type: WPA-PSK(no server)
Authentication: WPA-PSK + WPA2-PSK
Encryption Technique
Pre-shared Key (PSK): in[redacted]

159.149.[redacted]/wireless_wps_enabled.htm

Apps | SpiderFoot | OSINT | OSINT Tool | Mobile PT Tool | BooleServerGuide | Minosse - VAPT | Scadenziario

BELKIN. Router Setup

Wireless
Channel and SSID
Security
Guest Access
WPS
Use as Access Point
MAC Address Control
Utilities

Wireless > Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS): Enabled

Wi-Fi Protected Setup (WPS) is the industry standard method to simplify the security setup and management of Wi-Fi networks. You now can easily setup and connect to a WPA-enabled 802.11 network with WPS-certified devices using either Persional Information Number(PIN) method or Push Button Configuration(PBC) method. Legacy devices without WPS can be added to the network using the traditional manual configuration method.

Push and hold the PBC button on your Router for 3 seconds. Then start PBC on the device you want to connect to the Router within 2 minutes.

Start PBC

3)Manual Configuration Method

For client devices without WPS, manually configure the device with the following settings:

231/01 reato informatico

- Uso improprio delle risorse universitarie
- Collegamento anonimo alla rete wifi