FIRENZE TECNOLOGIA

OpenPrivacy: Software Libero per facilitare le PMI/PA nel processo di adeguamento al D.lgs 196/03

Eprivacy 2005, Firenze, 27 maggio 2005
Ivano Greco – Firenze Tecnologia, Azienda Speciale della CCIAA

FIRENZE TECNOLOGIA

Progetto Sicurezza Informatica

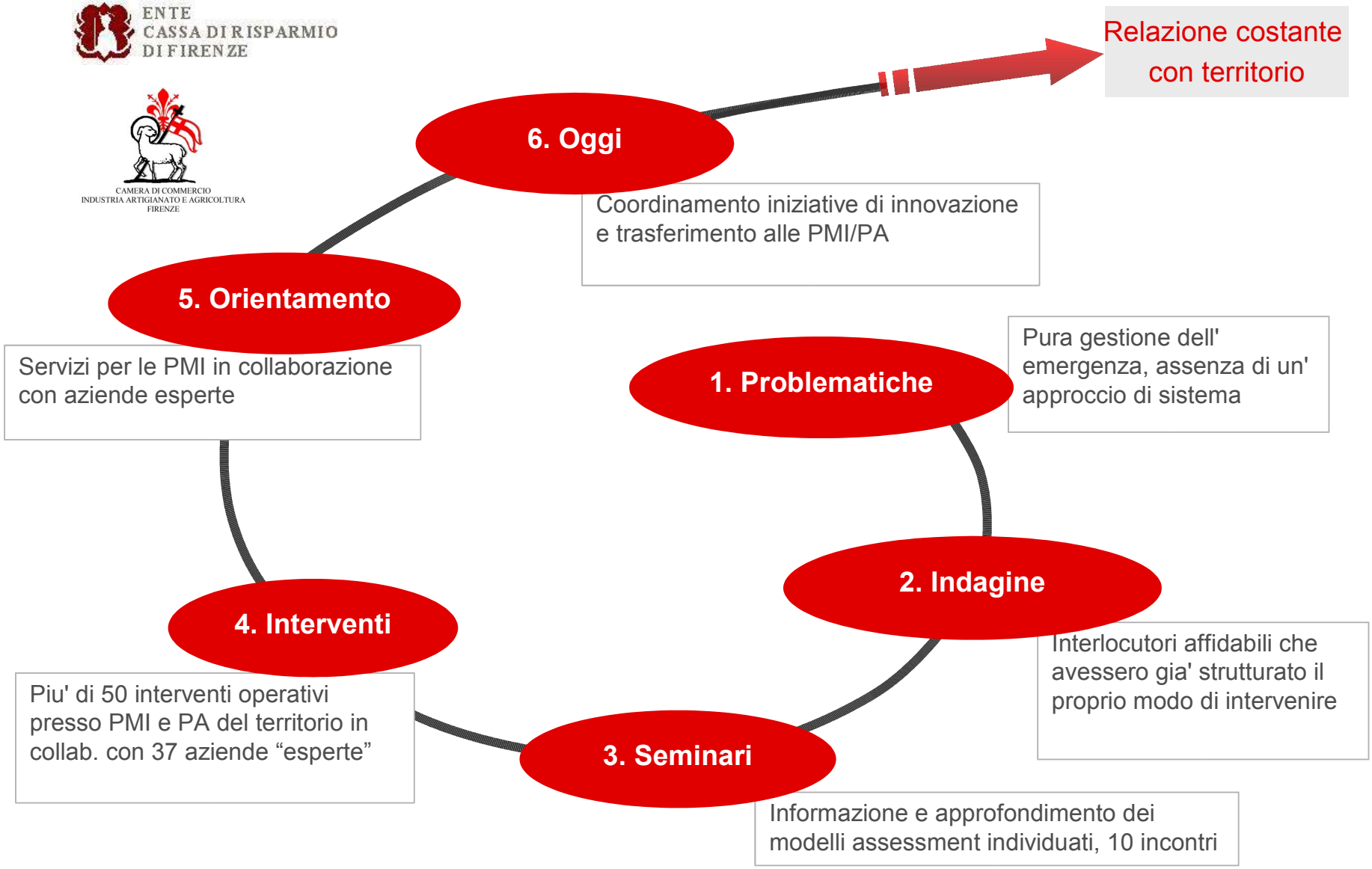
2002-2005

FIRENZE TECNOLOGIA

ENTE CASSA DI RISPARMIO DI FIRENZE

CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA FIRENZE

Intervento Sicurezza



FIRENZE TECNOLOGIA

Attivita' Principali

www.sicurinfo.it: arricchimento dei contenuti con inserimento di informazioni tematiche e di contributi delle aziende esperte.

- Disaster Recovery Plan

- Confronto fra ISO 9001: 2000 e BS 7799-2: 2002

- Il Processo di Analisi dei Rischi

Questionario Autovalutazione PMI: conformita' al D.lgs 196/03

Pubblicazione libretto: “La Sicurezza delle informazioni nelle PMI”

- “Lo standard di riferimento ISO/BS17799” (descrizione sintetica del processo per SGSI).

- “L'approccio metodologico” (semplificazione per le PMI)

- “La Sicurezza del Software” (Software Libero e Software Proprietario a confronto con la ISO17799)

OpenPrivacy: il Software Libero basato su Linux/Debian, Samba, LDAP, SQUID finalizzato a supportare le PMI nell'adeguamento alle Misure Minime di Sicurezza del D.lgs 196/03.

FIRENZE TECNOLOGIA

Il Processo di Assessment rispetto al D.lgs 196/03

FIRENZE TECNOLOGIA

Contesto Aziendale di riferimento

- ***Conoscitiva della società***
  - Raccogliere le informazioni in merito all'organizzazione che permettono di inquadrare la tipologia di impresa di cui si sta parlando, e in particolare le informazioni descritte di seguito. Tale raccolta di informazioni e la risposta alle domande poste permetteranno di presentare una documentazione in caso di verifica ispettiva da parte della Guardia di Finanza.
- ***L'attività***
  - Inserire una presentazione dell'azienda, dichiarare se fa parte di un gruppo, quali sono le sedi sul territorio, il numero dei dipendenti, l'**organizzazione interna** (corredata da organigramma/funzionigramma), specificare se l'azienda ha conseguito delle certificazioni riconosciute (ISO, SA ...altro) , il mercato di riferimento, le aree di business di cui si occupa.

FIRENZE TECNOLOGIA

Scenario di Riferimento

- ***Inventario beni aziendali***
  - Ciascun computer di proprietà dell'azienda deve essere inserito nell'inventario; per ciascun elaboratore (sia client, sia server) deve essere indicato il luogo di residenza fisica, devono essere elencati i software installati, e si deve individuare la persona cui è assegnato il bene aziendale.
- ***Identificazione banche dati e dei trattamenti***
  - Questa attività ha come fine il **censimento di tutte le banche dati** presenti e dei trattamenti effettuati su di esse da parte della società per verificare che esse vengano gestite in conformità alla legge ed esplorare la necessità di un'eventuale notificazione al Garante.
- ***Banche dati gestite senza e con l'ausilio di strumenti elettronici***
  - Descrivere il processo principale di gestione delle informazioni in azienda (approvvigionamento, vendita, gestione delle paghe ... etc... etc) In senso estensivo, sarebbe necessario descrivere tutti i processi che trattano le informazioni, così da avere più semplicità nell'elencare le banche dati.

FIRENZE TECNOLOGIA

Analisi del Rischio

- Analisi del Rischio: il metodo con cui si svolge l'analisi del rischio deve essere documentato, ripetibile, chiaro, si deve dimostrare di gestire il rischio; le scelte di gestione del rischio devono essere contestualizzate all'organizzazione.
  - Identificazione delle **minacce** e probabilita' di accadimento
  - Identificazione delle **vulnerabilita'**
  - Stima dell'**impatto** (considerando l'assenza di contromisure)
  - Definizione della Politica di **gestione del rischio**
- I parametri da tenere sotto controllo nell'analisi del rischio sono:
  - Confidenzialita' - assicurare che le informazioni siano accessibili solo a chi e' autorizzato
  - Integrita' – proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione
  - Disponibilita' – assicurare che gli utenti autorizzati possano effettivamente accedere alle informazioni e beni collegati nel momento in cui lo chiedono.

FIRENZE TECNOLOGIA

Gestione del Rischio

- Rischio = funzione (probabilita' minaccia* impatto* vulnerabilita')
- Stimato il Rischio si definiscono i controlli da applicare per ridurre il rischio a livelli accettabili per l'organizzazione
- La Gestione del Rischio
  - Contromisure tecnico / organizzative
  - Trasferimento del rischio
  - Accettare il rischio

FIRENZE TECNOLOGIA

Misure di Sicurezza

- Gestione delle Misure Minime di Sicurezza:
  Allegato B del D.lgs 196/03 per il trattamento di banche dati in formato elettronico
  - Sistemi di Autenticazione Informatica
  - Sistema di Autorizzazione
  - Altre misure di Sicurezza
  - Documento Programmatico sulla Sicurezza
  - Ulteriori misure in caso di trattamento di dati sensibili e giudiziari
- Identificazioni di Misure Idonee

FIRENZE TECNOLOGIA

OpenPrivacy: Software Libero

a supporto delle PMI / PA per l'adeguamento al D.lgs 196/03

FIRENZE TECNOLOGIA

Metodo Intervento

- Intervento di consulenza finalizzato alla produzione del DPSs
  - confronto fra il modello privacy nell'Ente e il modello previsto dal D.lgs 196/03 – TUP
    - organizzazione Ente
    - ruoli e responsabilita'
    - sistemi informativi e banche dati
    - analisi dei rischi
    - etc ... etc ...

- Piano di Sicurezza

PROBLEMATICHE SIMILI

FIRENZE TECNOLOGIA

Problematiche simili (1)

- Ambito: trattamento elettronico banche dati
  - dispersione delle banche dati (ciascun utente crea banche dati sul proprio PC senza regolamentazioni)
    - PC senza autenticazione/gestione politiche password se non inseriti in PDC (es. win98) --> dati in locale facilmente accessibili
    - Politiche di backup inesistenti
    - Etc ... etc...
  - presenza di un sistema applicativo server (procedure centralizzate Unix, AS400, etc..etc...)

FIRENZE TECNOLOGIA

Problematiche simili (2)

> Problematiche di base:

- gestione delle autenticazioni
- gestione delle profilazioni
- gestione delle politiche di password
- gestione di uno spazio disco condivisibile (FileServer)
- gestione dell'elenco aggiornato degli utenti e dei privilegi
- gestione delle operazioni di backup
- estensione autenticazione/profilazione per le connessioni ad internet degli utenti

> Altre problematiche:

- integrazione varie applicazioni Unix-like

FIRENZE TECNOLOGIA

Le Scelte

- Definizione delle caratteristiche del sistema (documento con le specifiche)
  - MMS --> funzionalita' OpenPrivacy
- Scelta della Licenza di distribuzione
  - Software Libero o Software Proprietario ?
  - I files di configurazione sono rilasciati con GNU/GPL
- Selezione delle “Aziende Esperte”
- Selezione dei moduli Software
  - Linux Debian, Samba, LDAP, SQUID.

FIRENZE TECNOLOGIA

Gruppo di Lavoro

- Truelite srl: http://www.truelite.it/

- Ing. Francesco Leoncino

- Libersoft: http://www.libersoft.it

- ComputerAssist: http://www.computerassist.it/

FIRENZE TECNOLOGIA

Funzionalita' OpenPrivacy

- Alcune funzionalita':
  - gestione delle autenticazioni (default 5 utenti)
  - gestione delle profilazioni (default 3 gruppi)
  - gestione dell'elenco aggiornato degli utenti e dei privilegi

- PDC per la gestione utenti e gruppi, amministrabile con intefaccia web-based
- Procedura per la creazione degli utenti, gruppi e assegnazione della prima password

FIRENZE TECNOLOGIA

Funzionalita' OpenPrivacy

> gestione delle politiche di password

politica default:

lunghezza password: 9 caratteri (Misura Sicurezza Idonea)

cambio password: avvertimento da parte del sistema e obbligo di cambio al termine del periodo previsto

primo utilizzo: il sistema richiede cambio password

FIRENZE TECNOLOGIA

Funzionalita' OpenPrivacy

- gestione di uno spazio disco condivisibile (FileServer)
- gestione delle operazioni di backup

finalita': definire le politiche di accesso alle banche dati e semplificare le operazioni di backup

FIRENZE TECNOLOGIA

Funzionalita' OpenPrivacy

- integrazione varie applicazioni Unix-like – LDAP
  - personalizzazione delle policy
  - scalabile in termini di utenze
  - integrabile anche in reti disomogenee

le valutazioni di integrazione devono essere svolte con appositi studi di integrazione

FIRENZE TECNOLOGIA

OpenPrivacy sul mercato

- Maggio 2005: Download 1400 - www.sicurinfo.it
  - Files di configurazione
  - Documentazione OpenPrivacy/Allegato B
- Domain Controller presso PMI e PA
- PAAS – Progetto Regione Toscana
- Corso di Formazione Giugno 2005 (richiesta voucher Regione Toscana)

FIRENZE TECNOLOGIA

Grazie per l'attenzione

Ivano Greco

i.greco@firenzetecnologia.it
http://www.sicurinfo.it

Eprivacy 2005, Firenze, 27 maggio 2005
Ivano Greco – Firenze Tecnologia, Azienda Speciale della CCIAA