# Sicurezza dei dati
# Protezione endpoint e gateway

BENASSI
systems management

La sicurezza necessita di attenzione : per questo motivo da molti anni lavoriamo per la centralizzazione e l'automazione delle soluzioni di controllo e allarme dei sistemi di protezione endpoint e gateway.

BENASSI
systems management

# Managed Data Security
La sicurezza inizia dalla prevenzione

## Introduzione

Esistono diversi approcci per garantire la sicurezza dei dati informatici. Il proibizionismo, guidato dalla volontà di eliminare le azioni intrinsecamente non sicure, ha un elevato impatto sul lavoro di tutti i giorni.
Il nostro progetto di infrastruttura sicura nasce dall'analisi di quelli che sono i consueti veicoli di infezione e di sottrazione non autorizzata di dati. Queste fonti e questi metodi sono sottoposti a procedimenti di analisi e conformità preventiva con il minore livello possibile di interazione con gli utenti.
A questo punto di vista si aggiunge la consapevolezza che la conoscenza di quello che avviene sui propri sistemi è un aspetto fondamentale per garantire la sicurezza.
Per questo, sempre in forma anonima per non violare la privacy degli utenti, viene gestita in ousourcing l'analisi delle tipologie di traffico web, di potenziale infezione, di attacco, etc.

## L'infrastruttura

L'attenzione delle proposte di sicurezza "on premise" si concentra sulla sicurezza endpoint e sulla sicurezza gateway. Quest' ultima include gli accessi Vpn e la gestione del traffico web. La sicurezza della posta elettronica è invece delegata ad appositi frontend esterni che proteggono i server dislocati nelle strutture dei clienti.
Come per le altre parti dell'infrastruttura erogata secondo il modello IaaS (Infrastructure as a Service) vengono centralizzate le attività di policing e reporting mentre rimane presso il cliente la parte attiva di software o apparati preposta a svolgere il lavoro di prevenzione e controllo. I vantaggi di questo modello sono molteplici, dal costante e puntuale livello di aggiornamento dei sistemi che non subiscono mai invecchiamento, all'elevatissimo livello di monitoraggio.
A seconda delle dimensioni della struttura da gestire è possibile scegliere la percentuale di outsourcing in modo da garantire l'ottimale sfruttamento delle risorse umane preposte alla gestione IT e delle infrastrutture di comunicazione.

## Le modalità di acquisto

La scalabilità è una caratteristica innata dei servizi erogati con il modello IaaS e SaaS (Software as a Service).
Nessun vincolo minimo, costi di setup assenti o irrisori, attivazione immediata, sono alcune caratteristiche che accomunano la maggior parte dei servizi che offriamo con il modello SaaS o IaaS. Nonostante questo non vi sono limiti alla scalabilità verso l'alto, con il pieno supporto per la progettazione del deployment in infrastrutture complesse.
Le caratteristiche vincenti di questo tipo di soluzioni sono l'efficienza tecnica e la scalabilità. Il vantaggio economico è solo un positivo effetto collaterale delle economie di scala.
Per i servizi che richiedono solo software il costo è un canone mentre se è richiesto hardware è possibile scegliere tra la soluzione totalmente in locazione e l'acquisto dell'hardware di proprietà con un canone per la gestione proattiva.

Microsoft Exchange Server 2010

### Sicurezza della posta elettronica

- Frontend per la sicurezza della posta
- Funzionalità di antispam
- Funzionalità di antivirus e antiphishing
- Quarantena gestibile dall'utente
- Quarantena gestibile dall'amministratore
- Funzionalità di Mail Relay
- Servizio SMTP autenticato
- Idoneo per Exchange e per qualsiasi server SMTP

TREND MICRO
Securing Your Journey to the Cloud

### Sicurezza a livello endpoint

- SIstemi antivirus Trend Micro OfficeScan
- Server OfficeScan gestito presso la sede cliente
- Server OfficeScan in datacenter
- Soluzione SAAS basata su Trend Micro OfficeScan
- Reportistica automatica centralizzata
- Fatturazione per anno solare o frazioni
- Nessuna procedura per il rinnovo di licenza
- Configurazione adatta a postazioni mobili
- Configurazione specifica per server
- Console di accesso dedicata
- Servizio di analisi degli avvisi di infezione
- Gestione degli outbreak
- Consulenza per la gestione delle minacce
- Monitoraggio con agente a bordo macchina
- Deployment automatizzato
- Soluzioni per Data Leak Prevention

FORTINET

### Sicurezza a livello gateway

- Appliance UTM
- Funzionalità di Intrusion Prevention
- Funzionalità di Application Control
- Funzionalità di Web Filtering
- Funzionalità di Email Filtering
- Funzionalità di Data Leak Prevention
- Gestione VPN IPSEC e SSL
- Autenticazione su LDAP, Radius, etc.
- Reportistica automatica centralizzata
- Monitoraggio Netflow, Jflow, Syslog, SNMP

Sede in Via del Commercio, 23 – 38121 - TRENTO (TN)
Tel. 0039-0461-825060 - Fax 0039-0461-825426
http://www.benassi.net – info@gruppobenassi.com