introduzione

Alessandro Armando

Laboratorio di sicurezza informatica (CSec)
DIBRIS, Università di Genova

Sicurezza del computer

Contorno

In cui si? Da tutte le parti!

Informatica: La rete è il computer!

Deve garantire l'accesso selettivo a macchine, programmi, dati, risorse computazionali, ecc.
Privacy di dati, attività, ...

Bancario: Bancomat, home banking, ecc.

Accesso ai conti, integrità dei dati, non ripudio delle transazioni, . . .

Telecomunicazioni: ad es. reti mobili (GSM)

Riservatezza della comunicazione, informazioni sulla posizione, . . .

(E-)Governo: governo in linea!

Contorno

Informazioni di sicurezza

- **Sicurezza del computer** si occupa della prevenzione e rilevazione di azioni non autorizzate da parte degli utenti di un sistema informatico.
  - **Autorizzazione** è centrale nella definizione.
  - Sensibile solo rispetto a a **politica di sicurezza**, indicando chi (o cosa) può eseguire quali azioni.
- **Informazioni di sicurezza** è ancora più generale. Ha a che fare con**informazione** indipendente da **sistemi informatici**.
  Nota che le informazioni sono più generali dei dati. I dati trasmettono informazioni. Ma le informazioni possono anche essere rivelate, senza rivelare dati, ad esempio mediante riepiloghi statistici.
- Costituisce un diritto fondamentale: la protezione di sé (possesso, ...).

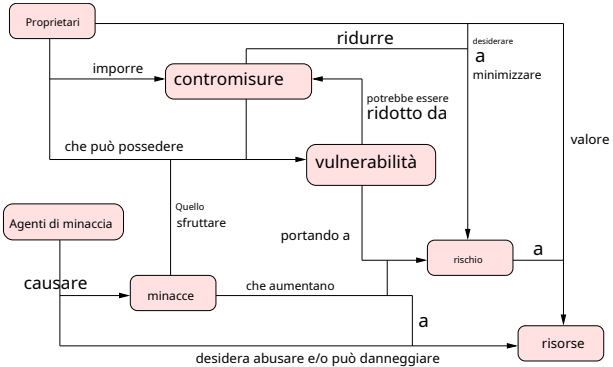
Sicurezza delle informazioni: concetti chiave

- La sicurezza riguarda la protezione di **risorse** a partire dal **minacce**.
  Le minacce sono il potenziale per l'abuso dei beni.
- **Proprietari** valorizzano i loro beni e vogliono proteggerli.**Agenti di minaccia** valutano anche i beni e cercano di abusarne.
- I proprietari analizzano le minacce per determinare quali si applicano; queste sono le**rischi** che può essere costato. Questo aiuta la selezione di**contromisure**, che riducono il**vulnerabilità**.

- Le vulnerabilità possono rimanere, lasciando qualche rischio residuo; i proprietari cercano di ridurre al minimo tale rischio, entro altri vincoli (fattibilità, spesa).

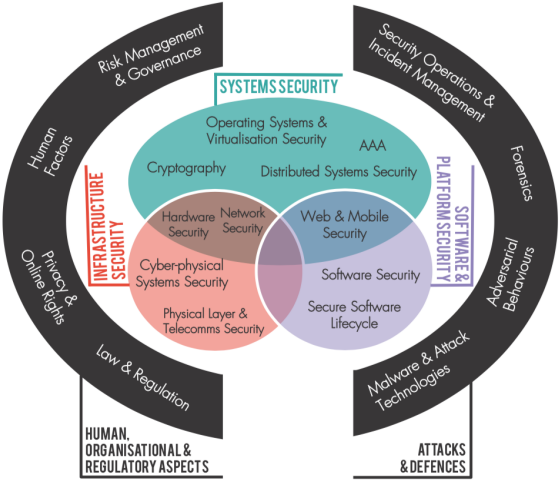
Nota: le minacce possono provenire da attività umane dannose o accidentali; di solito ci concentriamo su attività dannose.

Sicurezza delle informazioni: concetti chiave



- La classificazione descrive concetti e interrelazioni fondamentali.
- La policy (qui implicita) definisce le azioni autorizzate sui beni, ovvero ciò che costituisce abuso.

Il corpo di conoscenze sulla sicurezza informatica (www.cybok.org)



Contorno

Proprietà di sicurezza

riservatezza	*le informazioni non vengono apprese da mandanti non autorizzati*
integrità	*non sono stati (maliziosamente) alterati i responsabili o l'origine dei dati*
autenticazione	*possono essere identificati con precisione è possibile accedere ai dati/*
disponibilità	*servizi quando le azioni desiderate possono essere ricondotte ai*
responsabilità	*responsabili responsabili*

- Di solito vogliamo proteggere tutte le proprietà in modi specifici.
- Diversi meccanismi possono essere utilizzati per fornire protezione, ma fin dall'inizio dobbiamo renderci conto che **la sicurezza è un problema dell'intero sistema**.
- L'intero sistema è utilizzato nel senso più inclusivo: software, hardware, ambiente fisico, personale, strutture aziendali e legali.

Proprietà di sicurezza

riservatezza	*le informazioni non vengono apprese da responsabili non autorizzati i*
integrità	*dati non sono stati (malintenzionalmente) alterati*
autenticazione	*i mandanti o l'origine dei dati possono essere identificati con*
disponibilità	*precisione è possibile accedere ai dati/servizi quando le azioni*
responsabilità	*desiderate possono essere ricondotte ai mandanti responsabili*

- Di solito vogliamo proteggere tutte le proprietà in modi specifici.
- Diversi meccanismi possono essere utilizzati per fornire protezione, ma fin dall'inizio dobbiamo renderci conto che **la sicurezza è un problema dell'intero sistema**.
- L'intero sistema è utilizzato nel senso più inclusivo: software, hardware, ambiente fisico, personale, strutture aziendali e legali.

Proprietà di sicurezza

riservatezza	*le informazioni non vengono apprese da responsabili non autorizzati i*
integrità	*dati non sono stati (malintenzionalmente) alterati*
autenticazione	*i mandanti o l'origine dei dati possono essere identificati con*
disponibilità	*precisione è possibile accedere ai dati/servizi quando le azioni*
responsabilità	*desiderate possono essere ricondotte ai principali responsabili*

- Di solito vogliamo proteggere tutte le proprietà in modi specifici.
- Diversi meccanismi possono essere utilizzati per fornire protezione, ma fin dall'inizio dobbiamo renderci conto che **la sicurezza è un problema dell'intero sistema**.
- L'intero sistema è utilizzato nel senso più inclusivo: software, hardware, ambiente fisico, personale, strutture aziendali e legali.

Proprietà di sicurezza

riservatezza	*le informazioni non vengono apprese da responsabili non autorizzati i*
integrità	*dati non sono stati (malintenzionalmente) alterati*
autenticazione	*i mandanti o l'origine dei dati possono essere identificati con*
disponibilità	*precisione i dati/servizi sono accessibili quando lo si desidera*
responsabilità	*le azioni possono essere ricondotte a presidi responsabili*

- Di solito vogliamo proteggere tutte le proprietà in modi specifici.
- Diversi meccanismi possono essere utilizzati per fornire protezione, ma fin dall'inizio dobbiamo renderci conto che **la sicurezza è un problema dell'intero sistema**.
- L'intero sistema è utilizzato nel senso più inclusivo: software, hardware, ambiente fisico, personale, strutture aziendali e legali.

Proprietà di sicurezza

riservatezza	*le informazioni non vengono apprese da responsabili non autorizzati i*
integrità	*dati non sono stati (malintenzionalmente) alterati*
autenticazione	*i mandanti o l'origine dei dati possono essere identificati con*
disponibilità	*precisione è possibile accedere ai dati/servizi quando le azioni*
responsabilità	*desiderate possono essere ricondotte ai mandanti responsabili*

- Di solito vogliamo proteggere tutte le proprietà in modi specifici.
- Diversi meccanismi possono essere utilizzati per fornire protezione, ma fin dall'inizio dobbiamo renderci conto che **la sicurezza è un problema dell'intero sistema**.
- L'intero sistema è utilizzato nel senso più inclusivo: software, hardware, ambiente fisico, personale, strutture aziendali e legali.

Proprietà di sicurezza

riservatezza	*le informazioni non vengono apprese da responsabili non autorizzati i*
integrità	*dati non sono stati (malintenzionalmente) alterati*
autenticazione	*i mandanti o l'origine dei dati possono essere identificati con*
disponibilità	*precisione è possibile accedere ai dati/servizi quando le azioni*
responsabilità	*desiderate possono essere ricondotte ai mandanti responsabili*

- Di solito vogliamo proteggere tutte le proprietà in modi specifici.
- Diversi meccanismi possono essere utilizzati per fornire protezione, ma fin dall'inizio dobbiamo renderci conto che **la sicurezza è un problema dell'intero sistema**.
- L'intero sistema è utilizzato nel senso più inclusivo: software, hardware, ambiente fisico, personale, strutture aziendali e legali.

Contromisure di protezione

- **Prevenzione.** Cerca di prevenire le violazioni della sicurezza attraverso la progettazione del sistema e impiegando tecnologie di sicurezza appropriate come difese.
  Ad esempio, l'utilizzo di un firewall per impedire l'accesso esterno alle intranet aziendali.
- **Rilevamento.** In caso di violazione della sicurezza, cerchiamo di assicurarci che venga rilevata. La registrazione e i MAC (hash dei file per rilevare l'alterazione) sono metodi di rilevamento primari, sebbene *rilevamento delle intrusioni* i sistemi che controllano attivamente gli intrusi sono più comuni.
- **Risposta.** In caso di violazione della sicurezza, dobbiamo rispondere o recuperare i beni. Le risposte vanno dal ripristino dei backup all'informazione delle parti interessate o delle forze dell'ordine.

Riservatezza, privacy e segretezza

Le informazioni non vengono apprese da presidi non autorizzati

- La riservatezza è talvolta caratterizzata come la lettura non autorizzata dei dati, se si considera **controllo di accesso** le misure. Ma in generale ci occupiamo dell'apprendimento non autorizzato di informazioni, che è più sottile da affrontare.
- La riservatezza presuppone una nozione di soggetto autorizzato, o più in generale, a **politica di sicurezza** dicendo chi o cosa può accedere ai nostri dati. La politica di sicurezza viene utilizzata per il controllo degli accessi.
- Qualche volta: *privacy* riguarda la riservatezza per gli individui, considerando che *segretezza* riguarda la riservatezza per le organizzazioni, come società commerciali o governi. La privacy è talvolta usata anche nel senso di *anonimato* , mantenere la propria identità privata.
- Esempi di violazioni: le tue cartelle cliniche sono ottenute da un datore di lavoro senza il tuo consenso.

Riservatezza, privacy e segretezza

Le informazioni non vengono apprese da presidi non autorizzati

- La riservatezza è talvolta caratterizzata come la lettura non autorizzata dei dati, se si considera **controllo di accesso** le misure. Ma in generale ci occupiamo dell'apprendimento non autorizzato di informazioni, che è più sottile da affrontare.
- La riservatezza presuppone una nozione di soggetto autorizzato, o più in generale, a **politica di sicurezza** dicendo chi o cosa può accedere ai nostri dati. La politica di sicurezza viene utilizzata per il controllo degli accessi.
- Qualche volta: *privacy* riguarda la riservatezza per gli individui, considerando che *segretezza* riguarda la riservatezza per le organizzazioni, come società commerciali o governi. La privacy è talvolta usata anche nel senso di *anonimato* , mantenere la propria identità privata.
- Esempi di violazioni: le tue cartelle cliniche sono ottenute da un datore di lavoro senza il tuo consenso.

Riservatezza, privacy e segretezza

Le informazioni non vengono apprese da presidi non autorizzati

- La riservatezza è talvolta caratterizzata come la lettura non autorizzata dei dati, se si considera **controllo di accesso** le misure. Ma in generale ci occupiamo dell'apprendimento non autorizzato di informazioni, che è più sottile da affrontare.
- La riservatezza presuppone una nozione di soggetto autorizzato, o più in generale, a **politica di sicurezza** dicendo chi o cosa può accedere ai nostri dati. La politica di sicurezza viene utilizzata per il controllo degli accessi.
- Qualche volta: *privacy* riguarda la riservatezza per gli individui, considerando che *segretezza* riguarda la riservatezza per le organizzazioni, come società commerciali o governi. La privacy è talvolta usata anche nel senso di *anonimato* , mantenere la propria identità privata.
- Esempi di violazioni: le tue cartelle cliniche sono ottenute da un datore di lavoro senza il tuo consenso.

Riservatezza, privacy e segretezza

Le informazioni non vengono apprese da presidi non autorizzati

- La riservatezza è talvolta caratterizzata come la lettura non autorizzata dei dati, se si considera **controllo di accesso** le misure. Ma in generale ci occupiamo dell'apprendimento non autorizzato di informazioni, che è più sottile da affrontare.
- La riservatezza presuppone una nozione di soggetto autorizzato, o più in generale, a **politica di sicurezza** dicendo chi o cosa può accedere ai nostri dati. La politica di sicurezza viene utilizzata per il controllo degli accessi.
- Qualche volta: *privacy* riguarda la riservatezza per gli individui, considerando che *segretezza* riguarda la riservatezza per le organizzazioni, come società commerciali o governi. La privacy è talvolta usata anche nel senso di *anonimato* , mantenere la propria identità privata.
- Esempi di violazioni: le tue cartelle cliniche sono ottenute da un datore di lavoro senza il tuo consenso.

Integrità

I dati non sono stati alterati intenzionalmente

- L'integrità ha significati più generali altrove, ma nella sicurezza informatica ci preoccupiamo di prevenire l'eventuale alterazione dannosa dei dati, da parte di qualcuno che non è autorizzato a farlo.
- L'integrità in questo senso può essere caratterizzata come la scrittura non autorizzata di dati. Di nuovo, questo presuppone una politica di sicurezza che dice chi o cosa è autorizzato a modificare i dati.
- Esempio di violazione: un sistema di pagamento online altera un assegno elettronico per leggere 10.000 Euro invece di 100 Euro.

Integrità

I dati non sono stati alterati intenzionalmente

- L'integrità ha significati più generali altrove, ma nella sicurezza informatica ci preoccupiamo di prevenire l'eventuale alterazione dannosa dei dati, da parte di qualcuno che non è autorizzato a farlo.
- L'integrità in questo senso può essere caratterizzata come la scrittura non autorizzata di dati. Di nuovo, questo presuppone una politica di sicurezza che dice chi o cosa è autorizzato a modificare i dati.
- Esempio di violazione: un sistema di pagamento online altera un assegno elettronico per leggere 10.000 Euro invece di 100 Euro.

Integrità

I dati non sono stati alterati intenzionalmente

- L'integrità ha significati più generali altrove, ma nella sicurezza informatica ci preoccupiamo di prevenire l'eventuale alterazione dannosa dei dati, da parte di qualcuno che non è autorizzato a farlo.
- L'integrità in questo senso può essere caratterizzata come la scrittura non autorizzata di dati. Di nuovo, questo presuppone una politica di sicurezza che dice chi o cosa è autorizzato a modificare i dati.
- Esempio di violazione: un sistema di pagamento online altera un assegno elettronico per leggere 10.000 Euro invece di 100 Euro.

Autenticazione

Dati o servizi disponibili solo alle identità autorizzate

- L'autenticazione è la verifica dell'identità di una persona o di un sistema.
- Una qualche forma di autenticazione è un prerequisito se desideriamo consentire l'accesso a servizi o dati ad alcune persone ma negare l'accesso ad altre, utilizzando un sistema di controllo degli accessi.
- I metodi per l'autenticazione sono spesso caratterizzati come:
  - **qualcosa che hai**, ad esempio una tessera d'ingresso,**qualcosa che sai**, ad
  - esempio una password o una chiave segreta, oppure**qualcosa che sei**, ad es.
  - impronta digitale, firma, dati biometrici.
- Inoltre, dove ti trovi può essere controllato implicitamente o esplicitamente. Diversi metodi possono essere combinati per una maggiore sicurezza.
- Esempi di violazione: fingere di essere qualcun altro (furto di identità) falsificando e-mail o rubando credenziali.

Autenticazione

Dati o servizi disponibili solo alle identità autorizzate

- L'autenticazione è la verifica dell'identità di una persona o di un sistema.
- Una qualche forma di autenticazione è un prerequisito se desideriamo consentire l'accesso a servizi o dati ad alcune persone ma negare l'accesso ad altre, utilizzando un sistema di controllo degli accessi.
- I metodi per l'autenticazione sono spesso caratterizzati come:
  - **qualcosa che hai**, ad esempio una tessera d'ingresso,**qualcosa che sai**, ad
  - esempio una password o una chiave segreta, oppure**qualcosa che sei**, ad es.
  - impronta digitale, firma, dati biometrici.
- Inoltre, dove ti trovi può essere controllato implicitamente o esplicitamente. Diversi metodi possono essere combinati per una maggiore sicurezza.
- Esempi di violazione: fingere di essere qualcun altro (furto di identità) falsificando e-mail o rubando credenziali.

Autenticazione

Dati o servizi disponibili solo alle identità autorizzate

- L'autenticazione è la verifica dell'identità di una persona o di un sistema.
- Una qualche forma di autenticazione è un prerequisito se desideriamo consentire l'accesso a servizi o dati ad alcune persone ma negare l'accesso ad altre, utilizzando un sistema di controllo degli accessi.
- I metodi per l'autenticazione sono spesso caratterizzati come:
  - **qualcosa che hai**, ad esempio una tessera d'ingresso,**qualcosa che sai**, ad
  - esempio una password o una chiave segreta, oppure**qualcosa che sei**, ad es.
  - impronta digitale, firma, dati biometrici.
- Inoltre, dove ti trovi può essere controllato implicitamente o esplicitamente. Diversi metodi possono essere combinati per una maggiore sicurezza.
- Esempi di violazione: fingere di essere qualcun altro (furto di identità) falsificando e-mail o rubando credenziali.

Autenticazione

Dati o servizi disponibili solo alle identità autorizzate

- L'autenticazione è la verifica dell'identità di una persona o di un sistema.
- Una qualche forma di autenticazione è un prerequisito se desideriamo consentire l'accesso a servizi o dati ad alcune persone ma negare l'accesso ad altre, utilizzando un sistema di controllo degli accessi.
- I metodi per l'autenticazione sono spesso caratterizzati come:
  - **qualcosa che hai**, ad esempio una tessera d'ingresso,**qualcosa che sai**, ad
  - esempio una password o una chiave segreta, oppure**qualcosa che sei**, ad es.
  - impronta digitale, firma, dati biometrici.
- Inoltre, dove ti trovi può essere controllato implicitamente o esplicitamente. Diversi metodi possono essere combinati per una maggiore sicurezza.
- Esempi di violazione: fingere di essere qualcun altro (furto di identità) falsificando e-mail o rubando credenziali.

Autenticazione

Dati o servizi disponibili solo alle identità autorizzate

- L'autenticazione è la verifica dell'identità di una persona o di un sistema.
- Una qualche forma di autenticazione è un prerequisito se desideriamo consentire l'accesso a servizi o dati ad alcune persone ma negare l'accesso ad altre, utilizzando un sistema di controllo degli accessi.
- I metodi per l'autenticazione sono spesso caratterizzati come:
  - **qualcosa che hai**, ad esempio una tessera d'ingresso,**qualcosa che sai**, ad
  - esempio una password o una chiave segreta, oppure**qualcosa che sei**, ad es.
  - impronta digitale, firma, dati biometrici.
- Inoltre, dove ti trovi può essere controllato implicitamente o esplicitamente. Diversi metodi possono essere combinati per una maggiore sicurezza.
- Esempi di violazione: fingere di essere qualcun altro (furto di identità) falsificando e-mail o rubando credenziali.

Disponibilità

È possibile accedere a dati o servizi in modo affidabile e tempestivo

- Le minacce alla disponibilità riguardano molti tipi di eventi ambientali esterni (ad esempio, incendio, scollegamento della spina del server) nonché attacchi accidentali o dolosi nel software (ad esempio, infettare un sistema con un virus debilitante).
- Nella sicurezza informatica ci occupiamo della protezione contro il secondo tipo di minaccia, piuttosto che fornire forme più generali di tolleranza d'errore o garanzia di affidabilità.
- Garantire la disponibilità significa prevenire **negazione del servizio** (DoS), per quanto possibile. È possibile correggere gli attacchi a protocolli difettosi, ma gli attacchi che esauriscono le risorse disponibili sono più difficili, poiché può essere difficile distinguere tra un attacco e un uso legittimo del servizio.
- Esempi di violazioni: i letali attacchi DoS (DDoS) distribuiti contro i servizi online; interferire con il routing IP.

Disponibilità

È possibile accedere a dati o servizi in modo affidabile e tempestivo

- Le minacce alla disponibilità riguardano molti tipi di eventi ambientali esterni (ad esempio, incendio, scollegamento della spina del server) nonché attacchi accidentali o dolosi nel software (ad esempio, infettare un sistema con un virus debilitante).
- Nella sicurezza informatica ci occupiamo della protezione contro il secondo tipo di minaccia, piuttosto che fornire forme più generali di tolleranza d'errore o garanzia di affidabilità.
- Garantire la disponibilità significa prevenire **negazione del servizio** (DoS), per quanto possibile. È possibile correggere gli attacchi a protocolli difettosi, ma gli attacchi che esauriscono le risorse disponibili sono più difficili, poiché può essere difficile distinguere tra un attacco e un uso legittimo del servizio.
- Esempi di violazioni: i letali attacchi DoS (DDoS) distribuiti contro i servizi online; interferire con il routing IP.

Disponibilità

È possibile accedere a dati o servizi in modo affidabile e tempestivo

- Le minacce alla disponibilità riguardano molti tipi di eventi ambientali esterni (ad esempio, incendio, scollegamento della spina del server) nonché attacchi accidentali o dolosi nel software (ad esempio, infettare un sistema con un virus debilitante).
- Nella sicurezza informatica ci occupiamo della protezione contro il secondo tipo di minaccia, piuttosto che fornire forme più generali di tolleranza d'errore o garanzia di affidabilità.
- Garantire la disponibilità significa prevenire **negazione del servizio** (DoS), per quanto possibile. È possibile correggere gli attacchi a protocolli difettosi, ma gli attacchi che esauriscono le risorse disponibili sono più difficili, poiché può essere difficile distinguere tra un attacco e un uso legittimo del servizio.
- Esempi di violazioni: i letali attacchi DoS (DDoS) distribuiti contro i servizi online; interferire con il routing IP.

Disponibilità

È possibile accedere a dati o servizi in modo affidabile e tempestivo

- Le minacce alla disponibilità riguardano molti tipi di eventi ambientali esterni (ad esempio, incendio, scollegamento della spina del server) nonché attacchi accidentali o dolosi nel software (ad esempio, infettare un sistema con un virus debilitante).
- Nella sicurezza informatica ci occupiamo della protezione contro il secondo tipo di minaccia, piuttosto che fornire forme più generali di tolleranza d'errore o garanzia di affidabilità.
- Garantire la disponibilità significa prevenire **negazione del servizio** (DoS), per quanto possibile. È possibile correggere gli attacchi a protocolli difettosi, ma gli attacchi che esauriscono le risorse disponibili sono più difficili, poiché può essere difficile distinguere tra un attacco e un uso legittimo del servizio.
- Esempi di violazioni: i letali attacchi DoS (DDoS) distribuiti contro i servizi online; interferire con il routing IP.

Responsabilità

Le azioni sono registrate e possono essere ricondotte al responsabile

- Se i metodi di prevenzione e i controlli di accesso falliscono, possiamo ricorrere al rilevamento: mantenere un *percorso di controllo sicuro* è importante affinché le azioni che incidono sulla sicurezza possano essere ricondotte al responsabile.
- Una forma più forte di responsabilità è *non ripudio*, quando una parte non può in seguito negare un'azione.
- Creare un audit trail con i log della macchina è un problema spinoso: se un sistema è compromesso, anche i log possono essere manomessi. I modi per aggirare questo problema sono inviare messaggi di registro a un file di sola aggiunta, a un server separato o persino a una stampante fisicamente isolata.
- Esempio di violazione: un audit trail viene manomesso, perso o non è in grado di stabilire dove si è verificata una violazione della sicurezza.

Responsabilità

Le azioni sono registrate e possono essere ricondotte al responsabile

- Se i metodi di prevenzione e i controlli di accesso falliscono, possiamo ricorrere al rilevamento: mantenere un *percorso di controllo sicuro* è importante affinché le azioni che incidono sulla sicurezza possano essere ricondotte al responsabile.
- Una forma più forte di responsabilità è *non ripudio*, quando una parte non può in seguito negare un'azione.
- Creare un audit trail con i log della macchina è un problema spinoso: se un sistema è compromesso, anche i log possono essere manomessi. I modi per aggirare questo problema sono inviare messaggi di registro a un file di sola aggiunta, a un server separato o persino a una stampante fisicamente isolata.
- Esempio di violazione: un audit trail viene manomesso, perso o non è in grado di stabilire dove si è verificata una violazione della sicurezza.

Responsabilità

Le azioni sono registrate e possono essere ricondotte al responsabile

- Se i metodi di prevenzione e i controlli di accesso falliscono, possiamo ricorrere al rilevamento: mantenere un *percorso di controllo sicuro* è importante affinché le azioni che incidono sulla sicurezza possano essere ricondotte al responsabile.
- Una forma più forte di responsabilità è *non ripudio*, quando una parte non può in seguito negare un'azione.
- Creare un audit trail con i log della macchina è un problema spinoso: se un sistema è compromesso, anche i log possono essere manomessi. I modi per aggirare questo problema sono inviare messaggi di registro a un file di sola aggiunta, a un server separato o persino a una stampante fisicamente isolata.

- Esempio di violazione: un audit trail viene manomesso, perso o non è in grado di stabilire dove si è verificata una violazione della sicurezza.

Responsabilità

Le azioni sono registrate e possono essere ricondotte al responsabile

- Se i metodi di prevenzione e i controlli di accesso falliscono, possiamo ricorrere al rilevamento: mantenere un *percorso di controllo sicuro* è importante affinché le azioni che incidono sulla sicurezza possano essere ricondotte al responsabile.
- Una forma più forte di responsabilità è *non ripudio*, quando una parte non può in seguito negare un'azione.
- Creare un audit trail con i log della macchina è un problema spinoso: se un sistema è compromesso, anche i log possono essere manomessi. I modi per aggirare questo problema sono inviare messaggi di registro a un file di sola aggiunta, a un server separato o persino a una stampante fisicamente isolata.

- Esempio di violazione: un audit trail viene manomesso, perso o non è in grado di stabilire dove si è verificata una violazione della sicurezza.

Contorno

Gestire la sicurezza: implementare una soluzione

- UN *analisi della sicurezza* esamina le minacce che mettono a rischio gli asset, quindi propone politiche e soluzioni a un costo adeguato.
- UN *modello di minaccia* documenta le possibili minacce a un sistema, immaginando tutte le vulnerabilità che potrebbero essere sfruttate.
- UN *valutazione del rischio* studia la probabilità di ogni minaccia nell'ambiente del sistema e assegna un valore di costo, per trovare i rischi.
- UN *politica di sicurezza* affronta le minacce e descrive un insieme coerente di *contromisure*.
- I costi delle contromisure vengono confrontati con i rischi e manipolati per fare un ragionevole compromesso.
- Questo permette a *soluzione di sicurezza* da progettare, implementando tecnologie appropriate a un costo adeguato. In parte questo è un esercizio di budgeting; ma è anche importante spendere gli sforzi nel posto giusto.

Gestire la sicurezza: implementare una soluzione

- UN *analisi della sicurezza* esamina le minacce che mettono a rischio gli asset, quindi propone politiche e soluzioni a un costo adeguato.
- UN *modello di minaccia* documenta le possibili minacce a un sistema, immaginando tutte le vulnerabilità che potrebbero essere sfruttate.
- UN *valutazione del rischio* studia la probabilità di ogni minaccia nell'ambiente del sistema e assegna un valore di costo, per trovare i rischi.
- UN *politica di sicurezza* affronta le minacce e descrive un insieme coerente di *contromisure*.
- I costi delle contromisure vengono confrontati con i rischi e manipolati per fare un ragionevole compromesso.
- Questo permette a *soluzione di sicurezza* da progettare, implementando tecnologie appropriate a un costo adeguato. In parte questo è un esercizio di budgeting; ma è anche importante spendere gli sforzi nel posto giusto.

Gestire la sicurezza: implementare una soluzione

- UN *analisi della sicurezza* esamina le minacce che mettono a rischio gli asset, quindi propone politiche e soluzioni a un costo adeguato.
- UN *modello di minaccia* documenta le possibili minacce a un sistema, immaginando tutte le vulnerabilità che potrebbero essere sfruttate.
- UN *valutazione del rischio* studia la probabilità di ogni minaccia nell'ambiente del sistema e assegna un valore di costo, per trovare i rischi.
- UN *politica di sicurezza* affronta le minacce e descrive un insieme coerente di *contromisure*.
- I costi delle contromisure vengono confrontati con i rischi e manipolati per fare un ragionevole compromesso.
- Questo permette a *soluzione di sicurezza* da progettare, implementando tecnologie appropriate a un costo adeguato. In parte questo è un esercizio di budgeting; ma è anche importante spendere gli sforzi nel posto giusto.

Gestire la sicurezza: implementare una soluzione

- UN *analisi della sicurezza* esamina le minacce che mettono a rischio gli asset, quindi propone politiche e soluzioni a un costo adeguato.
- UN *modello di minaccia* documenta le possibili minacce a un sistema, immaginando tutte le vulnerabilità che potrebbero essere sfruttate.
- UN *valutazione del rischio* studia la probabilità di ogni minaccia nell'ambiente del sistema e assegna un valore di costo, per trovare i rischi.
- UN *politica di sicurezza* affronta le minacce e descrive un insieme coerente di *contromisure*.
- I costi delle contromisure vengono confrontati con i rischi e manipolati per fare un ragionevole compromesso.
- Questo permette a *soluzione di sicurezza* da progettare, implementando tecnologie appropriate a un costo adeguato. In parte questo è un esercizio di budgeting; ma è anche importante spendere gli sforzi nel posto giusto.

Gestire la sicurezza: implementare una soluzione

- UN *analisi della sicurezza* esamina le minacce che mettono a rischio gli asset, quindi propone politiche e soluzioni a un costo adeguato.
- UN *modello di minaccia* documenta le possibili minacce a un sistema, immaginando tutte le vulnerabilità che potrebbero essere sfruttate.
- UN *valutazione del rischio* studia la probabilità di ogni minaccia nell'ambiente del sistema e assegna un valore di costo, per trovare i rischi.
- UN *politica di sicurezza* affronta le minacce e descrive un insieme coerente di *contromisure*.
- I costi delle contromisure vengono confrontati con i rischi e manipolati per fare un ragionevole compromesso.
- Questo permette a *soluzione di sicurezza* da progettare, implementando tecnologie appropriate a un costo adeguato. In parte questo è un esercizio di budgeting; ma è anche importante spendere gli sforzi nel posto giusto.

Gestire la sicurezza: implementare una soluzione

- UN *analisi della sicurezza* esamina le minacce che mettono a rischio gli asset, quindi propone politiche e soluzioni a un costo adeguato.
- UN *modello di minaccia* documenta le possibili minacce a un sistema, immaginando tutte le vulnerabilità che potrebbero essere sfruttate.
- UN *valutazione del rischio* studia la probabilità di ogni minaccia nell'ambiente del sistema e assegna un valore di costo, per trovare i rischi.
- UN *politica di sicurezza* affronta le minacce e descrive un insieme coerente di *contromisure*.
- I costi delle contromisure vengono confrontati con i rischi e manipolati per fare un ragionevole compromesso.
- Questo permette a *soluzione di sicurezza* da progettare, implementando tecnologie appropriate a un costo adeguato. In parte questo è un esercizio di budgeting; ma è anche importante spendere gli sforzi nel posto giusto.