Cyber | Security | Defence spazia tra tutte le tecnologie e i contesti coinvolti nel complesso mondo della sicurezza informatica, più comunemente la cybersecurity, analizzandone in maniera trasversale tutti gli ambiti di applicazione, interazione e sviluppo, e trattando gli elementi correlati: tecnici, tecnologici, organizzativi, economici, politici, giuridici, sociali e umani.

I testi proposti hanno sia un taglio didattico e tecnico-pratico che saggistico e divulgativo e sono destinati a molteplici interlocutori: istituti e università, enti e aziende di settore, appassionati e cultori della materia | #_3

CLAUDIO SANTO MALAVENDA
MASSIMO MONTANILE
STEFANO VOCI

La sicurezza del software

Guida alla progettazione e allo sviluppo

prefazione di Genny Tortora

SAGGI

Indice

Prefazione

La notevole crescita dei livelli di informatizzazione e di digitalizzazione delle informazioni nella società moderna pone forte l'esigenza di garanzie sulla sicurezza dei processi e dei sistemi. La "sicurezza del software" descrive metodologie, framework, processi e strategie atti a garantire la sicurezza dei sistemi informatici riducendo le vulnerabilità all'interno del software e dell'ambiente in cui viene eseguito. Gli approcci alla sicurezza del software sono spesso strutturati attorno a potenziali attacchi informatici maliziosi. La sicurezza del software mira quindi a identificare, proteggere e creare soluzioni per quelle vulnerabilità che pur non derivando necessariamente da attacchi malevoli, sono comunque dannose.

Risulta quindi necessario adottare pratiche di programmazione orientate allo sviluppo di software che tenga conto delle problematiche legate alla sicurezza in modo da garantire codice robusto, che gode di security by design.

La sicurezza del software mira quindi ad aumentare l'integrità del software testando e rafforzando il software nelle varie fasi e ambienti in cui si muove durante il ciclo di vita di sviluppo del software e dopo il suo rilascio. Un software ben ingegnerizzato continuerà a funzionare anche sotto attacco malevolo.

Quando un'azienda ignora i problemi di sicurezza, si espone al rischio. Enormi quantità di dati sensibili sono archiviati nelle applicazioni aziendali e questi dati potrebbero essere rubati in qualsiasi momento. Le aziende che investono poco nella sicurezza

rischiano di subire perdite finanziarie e di avere una reputazione danneggiata.

Inoltre, i governi stanno ora legiferando e applicando misure di protezione dei dati. Ad esempio, il GDPR dell'Unione europea richiede alle organizzazioni di integrare le garanzie di protezione dei dati nelle prime fasi di sviluppo. Ignorare questi requisiti può comportare sanzioni molto onerose.

La creazione di applicazioni sicure è importante quanto la scrittura di algoritmi di qualità e l'attenzione all'aspetto della sicurezza può determinare il successo di un prodotto software rispetto ai concorrenti.

Questo libro di Claudio Santo Malavenda, Massimo Montanile e Stefano Voci rappresenta una guida utile alla progettazione e allo sviluppo di software sicuro. Gli autori, la cui autorevolezza nel campo della cybersicurezza, dello sviluppo del software e della protezione dei dati deriva dalla notevole esperienza maturata sul campo nella loro professione, forniscono una panoramica completa dei diversi aspetti che durante il ciclo di vita del software interessano la sicurezza. Dopo aver descritto il quadro normativo europeo e gli standard di riferimento sulla cybersicurezza e sulla sicurezza delle comunicazioni, il testo introduce una tassonomia delle cyberminacce che favorisce un approccio a più livelli nell'adozione di tecniche per garantire la sicurezza di un sistema informatico. Vengono illustrate metodologie, tecniche, principi e best practices nello sviluppo di un software sicuro. Due capitoli sono dedicati allo standard Common Criteria for Information Technology Security Evaluation, del quale vengono descritte le rigorose quanto efficaci procedure di valutazione e di certificazione. Vengono infine forniti esempi reali e casi d'uso, come quello emblematico della firma digitale, che aiutano il lettore ad assimilare i concetti presentati.

Genny Tortora

Introduzione

La trasformazione digitale sta cambiando radicalmente e rapidamente il mondo. Portando con sé un profondo e irreversibile mutamento delle modalità di comunicazione e di scambio di dati e informazioni. Nuove minacce incombono e cittadini, consumatori, fornitori si trovano esposti a reati informatici sempre più numerosi e sofisticati. I player del digital single market[1], pur se con differenti finalità, condividono l'obiettivo comune di un ambiente digitale sicuro, indispensabile per sostenere un cambiamento etico, che porti benefici per tutti.

I prodotti immessi sul mercato e i servizi offerti sono indissolubilmente legati al software: in modo diretto, nei casi in cui il software è necessario al funzionamento del prodotto stesso o quando esso è funzionale all'erogazione del servizio, oppure in modo indiretto, nei casi in cui il software è utilizzato per il disegno, la progettazione, la realizzazione, il test del prodotto o per l'erogazione del servizio. In molti casi il software è esso stesso il prodotto.

1. La strategia digital single market (DSM) è stata adottata dalla Commissione europea Juncker il 6 maggio del 2015. La strategia DSM è illustrata in "*A digital single market in Europe – Bringing down barriers to unlock online opportunities,* European Commission – Directorate General for Communication Citizens' information, Luxembourg, Publications Office of the European Union, 2016, https://op.europa.eu/en/publication-detail/-/publication/01368318-4e3d-11e6-89bd-01aa75ed71a1. Questa pubblicazione fa parte di una serie che spiega cosa fa l'UE in diversi settori politici, perché l'UE è coinvolta e quali sono i risultati. Tali pubblicazioni sono consultabili online a questi indirizzi: http://europa.eu/pol/index_en.htm; http://europa.eu/!bY34KD.

La necessità di arrivare rapidamente sul mercato con un nuovo prodotto o servizio spesso va a discapito della qualità. Pur di acquisire un vantaggio sull'arena di mercato rispetto ai propri competitor, si privilegia il soddisfacimento dei soli requisiti funzionali del prodotto/servizio (P/S) rispetto ai componenti non funzionali, la cui piena implementazione ne risulta sacrificata, perché troppo onerosa in termini di tempo e costi. Il produttore che sposa quest'approccio lo segue anche nelle altre fasi del ciclo di vita del P/S: la risoluzione di malfunzionamenti software spesso è effettuata omettendo parzialmente o totalmente i test sul soddisfacimento di importanti requisiti non funzionali (reliability, implementation, legislative), afferenti a tutte le classi della tassonomia proposta da Sommerville[2].

Osserviamo al progressivo aumento del numero di sistemi critici[3] nei quali il software gioca un ruolo chiave. Molti sistemi complessi, dai sistemi medici alle infrastrutture di controllo dei trasporti e delle telecomunicazioni, dipendono infatti da un software che sia affidabile e di alta qualità. I malfunzionamenti di tali software, dovuti a errori di disegno/implementazione/utilizzo o causati da cybercrime[4], possono arrecare danni, an-

2. Cfr. I. Sommerville, *Software Engineering*, Pearson Education Limited, Harlow (Essex) 2016. Come vedremo infatti, ai fini del nostro lavoro sono particolarmente interessanti i requisiti di reliability, afferenti al prodotto, quelli di implementation, relativi ai requisiti organizzativi e quelli di legge (privacy e safety) per i requisiti esterni.

3. I sistemi critici sono quei sistemi i cui malfunzionamenti generano danni rilevanti, non accettabili. Cfr. M. Hinchey, L. Coyle, *Evolving Critical Systems: a Research Agenda for Computer-Based Systems*, «17th IEEE International Conference and Workshops on Engineering of Computer-Based Systems», University of Limerick Institutional Repository, Limerick 2010, pp. 430-435, che definiscono 4 differenti tipi di sistemi critici, in base ai danni causati da un loro malfunzionamento. Safety-critical: può provocare la morte, gravi lesioni personali o danni all'ambiente naturale; mission-critical: può portare a un'incapacità di raggiungere gli obiettivi del progetto; business-critical: può portare a perdita di affari o danni alla reputazione; security-critical: può portare alla perdita di dati sensibili a seguito di furto o per smarrimento accidentale.

4. Cfr. vocabolario Treccani online (https://www.treccani.it/enciclopedia/sicurezza): cybercrime <sàibëkraim> s. ingl., usato in italiano al maschile – Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema o colpendolo (rispettivamente, si parla di computer as a *tool* e computer as a *target*), https://www.treccani.it/enciclope-

che gravi e a volte letali. Sempre più si ricorre alle assicurazioni per la cybersicurezza per coprire i danni economici, il furto di identità, gli attentati alla sicurezza personale, gli attentati alla reputazione, per citare le più frequenti violazioni che possono derivare dal cybercrimine.

L'importanza della cybersicurezza è infatti richiamata, nelle conclusioni del Consiglio dell'Unione europea sul futuro digitale dell'Europa[5], quale componente essenziale di un mercato unico digitalizzato, in quanto garantisce la fiducia nelle tecnologie digitali e nel processo di trasformazione digitale.

Cos'è la sicurezza?

Secondo Treccani[6] la sicurezza è la condizione che rende e fa sentire di essere esente da pericoli, o che dà la possibilità di prevenire, eliminare o rendere meno gravi danni, rischi, difficoltà, evenienze spiacevoli.

Ottima definizione, che include aspetti tecnici ed emotivi. Tecnicamente si richiamano infatti concetti e principi che riportano al trattamento sistematico dei rischi, a partire dall'identificazione delle minacce, alla definizione e classificazione dei rischi, alla valutazione degli impatti, fino alla loro gestione.

Secondo G. Ziccardi[7] tre sono i componenti fondamentali per garantire un ambiente sicuro: hardware senza difetti, software senza difetti e essere umano senza difetti. Il terzo componente è senz'altro stato inserito per completezza teorica, al fine di inclu-

dia/cybercrime_%28Lessico-del-XXI-Secolo%29/#:~:text=cybercrime%20s.,e%20computer%20as%20a%20target). Ultima consultazione 1 febbraio 2021.

5. Cfr. EU, *Shaping Europe's digital future,* Publications Office of the European Commission, Luxembourg 2020.

6. Cfr. Treccani, *Vocabolario on line*. https://www.treccani.it/enciclopedia/sicurezza.

7. Cfr. G. Ziccardi, *Il giornalista hacker – Piccola guida per un uso sicuro e consapevole della tecnologia*, Marsilio, Venezia 2012. Giovanni Ziccardi è professore associato dell'Università degli Studi di Milano, Dipartimento di scienze giuridiche Cesare Beccaria, dove insegna filosofia del diritto.

dere nel loop tutti gli attori coinvolti. In effetti l'ambizione dell'assenza di difetti è utopistica per tutti i componenti considerati ma non volendo affrontare gli impatti del capitalismo del mercato digitale, che mette seriamente a rischio l'autonomia degli esseri umani, la solidarietà sociale, la democrazia[8], ci limitiamo qui ad approfondire gli aspetti tecnici connessi allo sviluppo di software sicuro. I modelli di progettazione, sviluppo e test qui proposti ben si applicano anche alla realizzazione di hardware sicuro, che è tale in quanto è security by design il software/firmware che ne consente l'utilizzo, nell'accezione di interesse per il nostro lavoro.

Le vulnerabilità del software (per software intendiamo i protocolli sviluppati per coprire i componenti della pila ISO/OSI, tranne il primo[9]) sono dunque continuamente sfruttate[10] per compiere cybercrimini dagli hacker, «che hanno trovato terreno fertile dall'impiego forzato ed estemporaneo di strumenti e modalità operative prima poco utilizzate o conosciute»[11], a causa della pandemia da SARS-CoV-2 che ha costretto le organizzazioni a ricorrere al cd. smart working.

Aumenta di conseguenza la richiesta di software sicuri, per una maggiore consapevolezza da parte dell'utente finale ma soprattutto per la capacità delle organizzazioni di stimare i costi derivanti da cybercrimini o da malfunzionamenti SW. Le organizzazioni più

8. Cfr. R.B. Reich, nella sua recensione a *Il capitalismo della sorveglianza – Il futuro dell'umanità nell'era dei nuovi poteri* di Shoshana Zuboff, trad. di P. Bassotti, LUISS University Press, 2019.

9. Il modello OSI (Open Systems Interconnection) dell'ISO (International Organization for Standardization), conosciuto anche come modello ISO/OSI, è lo standard stabilito nel 1984 per la definizione di un modello di riferimento *open* per l'interconnessione di sistemi. Tale standard è stato rivisto e confermato dalla ISO nel 2000. Di seguito l'elenco dei 7 livelli della pila ISO/OSI: 1. fisico (physical layer); 2. collegamento dati (datalink layer); 3. rete (network layer); 4. trasporto (transport layer); 5. sessione (session layer); 6. presentazione (presentation layer); 7. applicazione (application layer).

10. Secondo il *Rapporto Clusit* 2020, lo sfruttamento di vulnerabilità note è in leggera diminuzione (il valore 1H2020 è il 4% in meno rispetto al dato rilevato nello stesso periodo del 2019), mentre aumenta l'utilizzo di vulnerabilità "0-day", (il dato nel primo semestre 2020 ha fatto registrare un incremento del 16,7% rispetto al primo semestre 2019), https://clusit.it/rapporto-clusit/, ultima consultazione 8 gennaio 2021.

11. Tratto dall'introduzione al *Rapporto Clusit* 2020 sulla sicurezza ICT in Italia.

sensibili al tema hanno ben compreso che prevenire è meglio che curare.

Alcuni settori verticali (trasporti, finanza, aerospace&defence, sanità) considerano la sicurezza del software una priorità assoluta. La sicurezza ha un'importanza fondamentale anche per la pubblica amministrazione (PA), in quanto necessaria per garantire la disponibilità, l'integrità e la riservatezza delle informazioni proprie del sistema informativo della PA, come ben evidenziato nelle linee guida sulla sicurezza nello sviluppo SW, emesse dall'Agenzia per l'Italia digitale della Presidenza del Consiglio dei Ministri[12]. Progettare SW sicuro riducendo le vulnerabilità costituisce dunque, per le organizzazioni che operano in tali segmenti di mercato, un obiettivo primario. Un software sicuro, pur non potendo garantire la totale sicurezza del sistema su cui è impiegato, consente da una parte di rendere più difficile la vita agli hacker e dall'altra di mettere a disposizione un ambiente più sicuro all'utilizzatore, il quale, opportunamente formato e informato alla cultura del rischio e della sicurezza, potrà vivere più serenamente la propria user experience, agendo con le giuste cautele senza però doversi preoccupare di effettuare azioni particolari o complesse configurazioni SW per proteggersi, essendo il software stesso a garantire un ambiente digitale sicuro. La differenza rispetto ad ambienti digitali insicuri è notevole, poiché in tali ambienti insidiosi è l'utente a doversi guardare le spalle, spesso non avendo le competenze e dunque la reale capacità di farlo, se utilizza sistemi insecurity by design. Un utente che non fosse sollevato dalla necessità di doversi occupare di rendere sicuro l'ambiente digitale in cui opera è continuamente esposto a notevoli condizioni di stress, non sentendosi mai esente da pericoli. Ciò è peraltro strettamente connesso alla produttività dei lavoratori in smart working, con evidenti vantaggi da parte del datore di lavoro capace di assicurare device e tool sicuri al lavoratore. La consapevolezza dell'utente è tuttavia fondamentale e

12. Cfr. Agenzia per l'Italia digitale, *Linee guida di sicurezza nello sviluppo delle applicazioni – Ver. 1.0*, Presidenza del Consiglio dei ministri, Roma 2017.

la formazione continua sui temi della sicurezza costituisce un imprescindibile elemento di supporto alla cybersicurezza. La componente organizzativa, intesa come governance, responsabilità, ruoli, processi e la cooperazione tra organizzazioni, coordinata a livello europeo e extra UE costituisce un altro asset fondamentale. Qui ci limitiamo ad affrontare il tema della sicurezza del software.

I primi standard proposti per valutare la sicurezza dei dati gestiti da un sistema informatico risalgono ai primi anni ottanta[13], fino ad arrivare alla definizione dei common criteria[14], uno standard internazionale accettato e condiviso da più Stati per assicurare, tramite certificazione, che un prodotto soddisfa particolari requisiti di sicurezza, a fronte di una verifica da parte di laboratori di valutazione autorizzati e indipendenti.

L'impostazione rigorosa dei common criteria e la loro implementazione consente infatti di sviluppare software sicuri. Questo lavoro si propone come guida metodologica per definire i requisiti, progettare, sviluppare, testare e documentare un prodotto sicuro e in particolare compliance allo standard common criteria e fornisce indicazioni utili per velocizzare il processo di certificazione di tali prodotti.

13. Cfr. F. Montanile, M. Montanile, *Un modello per la sicurezza dei dati personali nell'era digitale*, tab edizioni, Roma 2020.

14. I common criteria sono divenuti standard internazionale ISO/IEC 15408-2 nel 1999.