spritzmatter

your cybersecurity partner for innovation

Cyber Security Posture

SPRITZ MATTER Srl Via Ugo Foscolo,3 - 35131 Padova (PD) - Italy - https://spritzmatter.com

Chi Siamo

Spritz Matter è una **spin-off** dell'Università di Padova ed una **startup innovativa** nata con l'obiettivo di sviluppare **soluzioni** avanzate ed all'**avanguardia** nel settore della **cybersecurity** offrendo servizi e prodotti di alta qualità per proteggere i sistemi informatici dai cyber attacchi. La nostra mission è creare un ambiente digitale sicuro per le aziende, proteggendo i loro dati e garantendo la continuità delle loro operazioni.

Siamo fortemente orientati all'utilizzo delle tecnologie innovative, come l'**intelligenza artificiale**. Il nostro background accademico e il continuo aggiornamento sulle ultime tendenze, ci permettono di analizzare i problemi con **metodo scientifico** e di sviluppare ed implementare tecnologie all'avanguardia per la rilevazione e la prevenzione avanzate delle minacce informatiche.

Il pericolo delle Minacce Informatiche

Gli autori di un **cyber attacco** mirano principalmente a causare disagio o **danni** alla vittima, con obiettivi che possono variare dal ricatto per estorcere denaro all'azienda, fino alla divulgazione di documenti sensibili per fini di spionaggio industriale, come nel caso delle aziende concorrenti.

Tra i cyber attacchi più comuni alle aziende vi sono:

- **Ransomware**: bloccano l'accesso ai componenti critici della rete, costringendo le aziende a pagare un riscatto per ripristinare l'accesso;
- **Malware**: installazione di software dannosi sui sistemi aziendali per sottrarre, alterare o distruggere dati sensibili;
- **Spyware**: attacchi per informazioni in modo subdolo, trasmettendo dati dal disco rigido senza il consenso dell'utente;
- **Attacchi DDoS (Distributed Denial of Service)**: sovraccaricano un sistema o una rete con traffico fittizio, rendendoli inaccessibili agli utenti legittimi.
- **Phishing**: ingannare gli utenti per ottenere informazioni sensibili, come credenziali di accesso, attraverso e-mail o messaggi di testo fraudolenti.

Il rapporto del 2023 dell'Associazione Italiana per la Sicurezza Informatica (Clusit) ha evidenziato un notevole **aumento** dei cyber **attacchi** in **Italia** rispetto al resto del mondo nel periodo 2019-2023. In particolare, in Italia si è registrato un aumento del **+300%**, mentre la media mondiale è stata del +60%. Le infrastrutture informatiche italiane sono dunque diventate un bersaglio allettante per gli attaccanti, e per questa ragione è cruciale adottare misure di sicurezza all'avanguardia per proteggerle.

Mappatura degli Asset Aziendali

La fase di **mappatura degli asset** nella cybersecurity è un passaggio cruciale che consente di identificare e valutare gli asset aziendali rilevanti ai fini dei requisiti di sicurezza informatica. Questo processo mira a mettere in luce l'esposizione di tali asset a vulnerabilità e minacce potenziali, rappresentando una fase preliminare essenziale per la valutazione dei rischi. Gli asset possono assumere forme diverse, comprese risorse fisiche, risorse umane e processi aziendali. Per quanto riguarda la sicurezza delle informazioni, gli asset rilevanti possono essere suddivisi principalmente in due categorie: asset primari e asset di supporto.

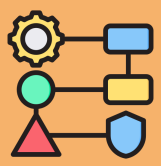
- Gli **asset primari** comprendono processi aziendali critici e attività, nonché informazioni vitali per la missione o il core business dell'azienda.
- Gli **asset di supporto** sono quegli elementi soggetti a vulnerabilità che, se compromessi, potrebbero danneggiare gli asset primari.

L'**inventario degli asset** fornisce una panoramica completa degli strumenti che costituiscono l'organizzazione e sono coinvolti nei vari processi aziendali. Questo inventario è essenziale per comprendere e controllare gli elementi che compongono un sistema di gestione per la sicurezza delle informazioni. Solo attraverso tale conoscenza è possibile determinare cosa è necessario proteggere e implementare le misure di sicurezza adeguate.

Cosa Offriamo?

SPRITZ Matter offre i seguenti servizi:

- **inventario**: definizione di un documento contenente i dispositivi informatici ed cyber-fisici dell'azienda.



Threat Modeling

Il Threat Modeling offre una panoramica dettagliata delle risorse che compongono l'azienda, come ad esempio le informazioni personali dei clienti. Esamina anche le minacce e le vulnerabilità connesse, sia interne al prodotto che nell'ambiente circostante, offrendo dettagli sulle strategie di mitigazione. Questo processo si rivela particolarmente fondamentale in vari scenari:

1. **Sviluppo di Software**: durante le fasi di design e sviluppo di un prodotto, il Threat Modeling può essere adottato come misura proattiva per identificare e mitigare potenziali minacce. Fornisce un'analisi sistematica dei controlli e delle difese necessari.
2. **Dopo il Rilascio di un Prodotto Software o Hardware**: come misura reattiva, il Threat Modeling può essere impiegato dopo il deploy di un prodotto per identificare e affrontare problemi inizialmente non previsti. Questo approccio supporta pratiche come ethical hacking, penetration testing, source code review e fuzz testing.
3. **Gestione dei Rischi Aziendali**: il Threat Modeling può essere utilizzato per elencare minacce che possono interrompere i processi aziendali, come terremoti, alluvioni o furti, e per individuare modi per contrastare o mitigare queste minacce.

Cosa Offriamo?

SPRITZ Matter offre i seguenti servizi:

- **sviluppo threat modeling** degli asset aziendali richiesti dall'azienda.

Vulnerability Assessment

Il **Vulnerability Assessment** rappresenta un processo continuo e periodico volto a definire, identificare, classificare e segnalare le vulnerabilità informatiche presenti negli asset aziendali. La sua importanza nella cybersecurity è evidente per diverse ragioni:

1. **Identificazione delle Vulnerabilità**: questa metodologia consente alle organizzazioni di comprendere le vulnerabilità presenti nei propri asset, facilitando la determinazione delle priorità per la loro mitigazione.

2. **Protezione dell'Impresa**: il Vulnerability Assessment svolge un ruolo cruciale nella protezione aziendale da violazioni di dati e altri attacchi informatici. Inoltre, contribuisce a garantire la conformità con normative rilevanti, come il Regolamento Generale sulla Protezione dei Dati (GDPR).

3. **Tipologie di Valutazioni**: Un processo completo di Vulnerability Assessment impiega diversi strumenti automatici per eseguire scansioni approfondite in tutto l'ambiente IT. Ciò consente di identificare vulnerabilità nelle applicazioni, dispositivi finali, carichi di lavoro, database e sistemi.

Si consiglia di condurre periodicamente un vulnerability assessment degli asset aziendali, considerando che gli ambienti IT sono in continua evoluzione con l'acquisizione di nuovi dispositivi e software. Le minacce informatiche emergenti rendono i sistemi aziendali sempre più esposti a potenziali attacchi cyber. Infine, per garantire la conformità alle normative sulla sicurezza informatica e sulla protezione dei dati, come il GDPR, è essenziale mantenere un adeguato livello di sicurezza, e il Vulnerability Assessment regolare risulta fondamentale per questo scopo.

Cosa Offriamo?

SPRITZ Matter offre i seguenti servizi:

- **Vulnerability Assessment - Infrastruttura:**
  - Identificazione di Minacce - Analisi approfondita per individuare potenziali vulnerabilità e minacce nell'infrastruttura aziendale.

  - Analisi del Traffico - Esame del traffico interno per rilevare flussi di comunicazione indesiderati o malevoli, contribuendo a una gestione più sicura della rete.

- **Vulnerability Assessment - Web App:** analisi specifica volta a individuare potenziali vulnerabilità e minacce legate alle applicazioni web dell'azienda. Questo servizio si concentra sulla sicurezza delle web app per prevenire exploit e violazioni.

- **Monitoraggio Ricorrente:** possibilità di definire le attività di Vulnerability Assessment in modalità periodica. Questo assicura che l'azienda rimanga costantemente aggiornata e protetta dalle ultime minacce cibernetiche.

Penetration Test

Un **Penetration Test** è un'esercitazione di sicurezza che simula un attacco informatico con l'obiettivo di individuare eventuali vulnerabilità in un sistema informatico. Questa attività è condotta da esperti di sicurezza, comunemente noti come ethical hackers, che impiegano strumenti e tecniche di hacking per identificare e risolvere le possibili vulnerabilità presenti nel sistema.

Il Penetration Test può coinvolgere l'intero sistema informatico di un'organizzazione, compresi software, applicazioni web, reti e altre risorse. Durante tale processo, i tester possono attivamente sfruttare i punti deboli individuati, consentendo al team di sicurezza di comprendere come veri hacker potrebbero sfruttare tali vulnerabilità per accedere a dati sensibili o interrompere le operazioni. La fase di penetration test può abbracciare diversi asset aziendali, che comprendono sia componenti hardware che software, oltre alla verifica della componente umana.

Penetration Test di Componenti Informatiche. Il penetration test è un'attività specializzata che si concentra sull'identificazione di potenziali criticità nelle componenti software o hardware di un asset aziendale specifico. A differenza di un classico Vulnerability Assessment, che fornisce una visione completa delle vulnerabilità di un sistema, il Penetration Test è si focalizza su come un singolo punto debole può essere sfruttato in un attacco.

Campagne di Phishing. Il phishing rappresenta una forma di frode informatica finalizzata al furto di dati sensibili, mascherandosi sotto l'apparenza di fonti affidabili. Questo processo si attua principalmente attraverso l'invio di email ingannevoli che mimano il nome o il logo di aziende conosciute, richiedendo alle vittime l'inserimento di dati personali. Una volta ottenute tali informazioni, gli hacker possono sfruttarle per attività illecite come furti di identità o pagamenti non autorizzati.

È importante notare che il phishing non si limita solo alle email, ma coinvolge sempre più frequentemente altri canali digitali come gli SMS, le chat di WhatsApp e i social network. Pertanto, la consapevolezza delle caratteristiche del phishing è cruciale per evitare di cadere nelle trappole di questi attacchi.

Cosa Offriamo?

SPRITZ Matter offre i seguenti servizi:

- **Penetration Test - Infrastruttura Rete**: attività che prevede di emulare un attaccante e compromettere l'infrastruttura aziendale, accedendo a dati sensibili o eseguendo operazioni non normalmente autorizzate;

- **Penetration Test - Web App:** attività che prevede di emulare un attaccante e compromettere la web app, accedendo a dati sensibili o eseguendo operazioni non normalmente autorizzate;

- **Penetration Test - AI App**: attività che prevede di emulare un attaccante per compromettere un servizio basato su AI (Artificial Intelligence) e manipolarne i risultati/operazioni;

- **Campagne di Phishing:** attività che prevede la simulazione di attacchi di phishing sui propri dipendenti. Puo' essere effettuata tramite tentativi di furto (simulando un vero e proprio attacco).

Miglioramento della Postura Cyber

La postura di sicurezza informatica di un'azienda, comunemente nota come "cybersecurity posture," rappresenta l'insieme delle misure, politiche e tecnologie implementate da un'organizzazione per mitigare i rischi informatici e preservare le risorse digitali. In altre parole, è la posizione di difesa che un'azienda adotta per proteggersi dagli attacchi cibernetici e garantire la sicurezza dei propri dati e sistemi. Migliorare la postura cyber di un'azienda implica l'adozione di un approccio olistico che coinvolge tecnologia, processi e risorse umane al fine di proteggere l'organizzazione da minacce informatiche e garantire la sicurezza dei dati e dei sistemi.

Cosa Offriamo?

SPRITZ Matter offre i seguenti servizi:

- **Sviluppo di Soluzioni Custom per il Miglioramento della Cybersecurity:** il nostro team è specializzato nello sviluppo di soluzioni su misura per affrontare le sfide della cybersecurity e dell'intelligenza artificiale. Utilizziamo un approccio di fast prototyping per sviluppare rapidamente Proof of Concept (PoC) e Minimum Viable Product (MVP);

- **Fix di Vulnerabilità**: offriamo un servizio di supporto per affrontare e risolvere le vulnerabilità identificate durante le attività di vulnerability assessment e penetration test per contribuisce a garantire la sicurezza continua dei sistemi;

Percorsi di sviluppo competenze cyber

L'incremento delle competenze dei propri dipendenti nell'ambito della cybersecurity rappresenta un primo passo fondamentale per rafforzare le difese aziendali. In questo documento, presentiamo la nostra proposta di sviluppo di competenze che abbraccia sia la cybersecurity che l'intelligenza artificiale. È da considerare l'espansione di questa lista ad altre aree tematiche specifiche nel campo della sicurezza informatica e dell'intelligenza artificiale.

Cosa Offriamo?

SPRITZ Matter offre i seguenti percorsi di sviluppo competenze:

Codice	Nome Modulo	Descrizione
	Cyber Security	
F1.1	Introduzione alla cyber security	Introduzione ai concetti base della cybersecurity.
F1.2	Cyber attacchi e cyber difese	Sessione di approfondimento delle principali cyber minacce e best practice sul come difendersi.
F1.3	Sicurezza Industriale	Approndimento del tema della cyber security in impianti industriali, i quali seguono paradigmi di difese diversi dalle reti IT classiche.
F1.4	Laboratorio di Phishing	Supporto all'identificazione dei mail di Phishing attraverso un laboratorio interattivo pratiche.
	Intelligenza Artificiale	
F2.1	Il ruolo dell'intelligenza artificiale nell'industria	Introduzione all'intelligenza artificiale, e come essa puo' venire adottata per scopi sia benevoli che malevoli in cyber security.
F2.2	Adversarial Machine Learning	Approfondimento del tema della sicurezza dell'Intelligenza Artificiale. Vengono trattate le principali famiglie di attacco a sistemi di AI.
F2.3	Addestramento all'utilizzo di copilot	Training pratico su strumenti di intelligenza artificiale come Copilot, per automatizzare compiti, ottimizzare processi e aumentare la produttività aziendale.

La Nostra Offerta

Codice	Nome Attività	Tempistiche
Mappatura degli Asset Aziendali		
A1.1	Inventario	4 settimane
Threat Modeling		
A2.1	Threat Modeling	1 - 2 mesi
Vulnerability Assessment		
A3.1	Vulnerability Assessment - Infrastruttura	4 settimane
A3.2	Vulnerability Assessment - Web App	4 settimane
A3.3	Monitoraggio ricorrente	TBD
Penetration Test		
A4.1	Penetration Test - Infrastruttura Rete	4 settimane
A4.2	Penetration Test - Web App	4 settimane
A4.3	Penetration Test - AI App	4 settimane
A4.4	Campagna di Phishing	1 mese
Miglioramento della Postura Cyber		
A5.1	Sviluppo di Soluzioni Custom per il Miglioramento della Cybersecurity	oraria
A5.2	Fix di vulnerabilità	oraria
Percorsi di sviluppo competenze Cyber		
A6.1	Percorso di sviluppo competenze cyber in base alle necessità del cliente.	oraria

Nella seguente tabella vengono sintetizzate le attività di cyber security offerte dal nostro team di esperti. Le tempistiche possono variare in base alle specifiche esigenze del cliente.