WORKSHOP GARR 2024

NET MAKERS

Distributed Accountability

Un approccio organizzativo al *Cybersecurity Rating*

Enrico Venuto

Politecnico di Torino

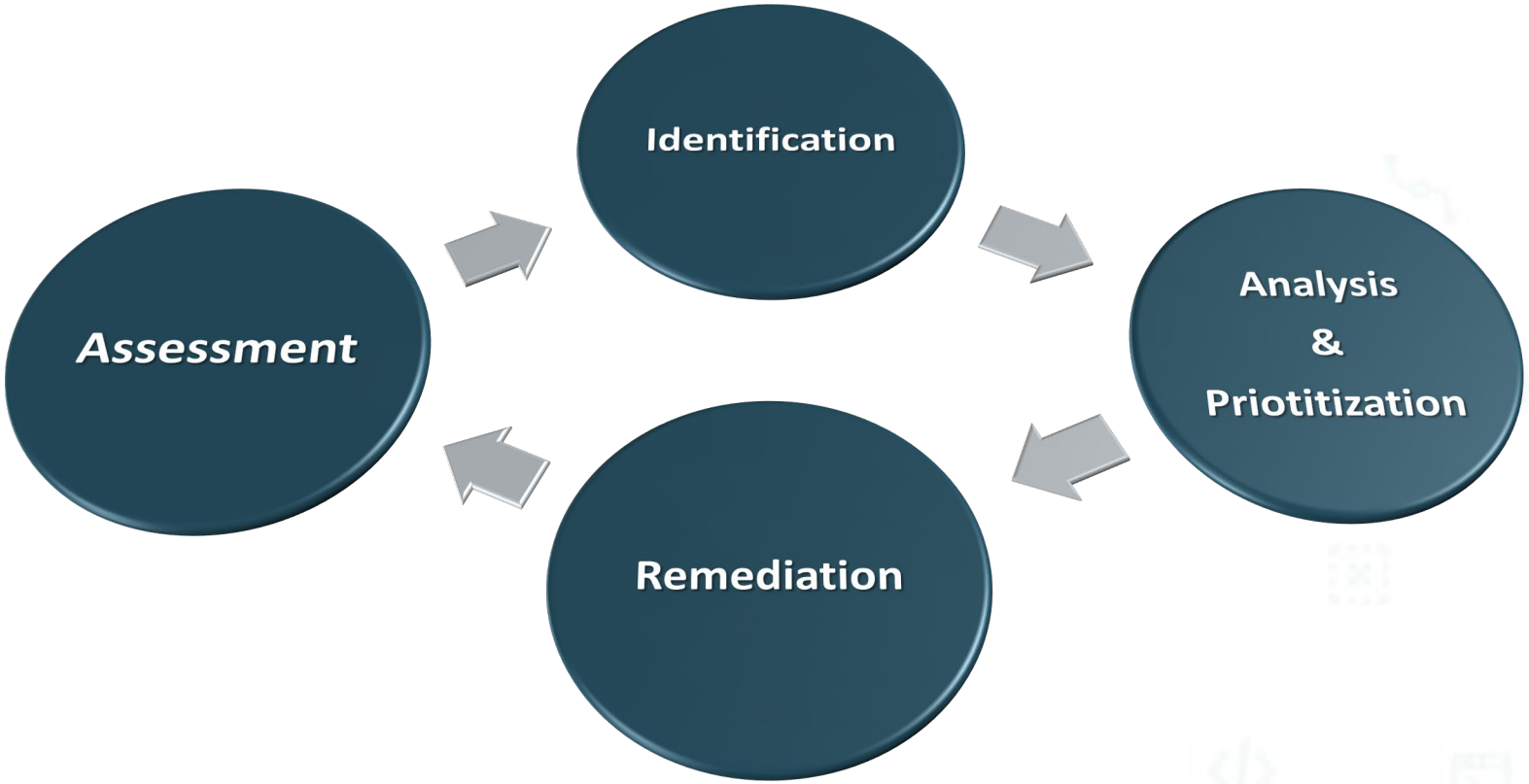
Politecnico di Torino

Vulnerability Assessment

Tradizionalmente basato su
- Approccio White Box
- Self-Operated
- Asset conosciuti
- Web security assessment

In alcuni casi
- Commissionato all'esterno
- Approccio Grey/Black Box
- Penetration testing

…e le sedi remote?
… e il cloud?



Attack Surface management

Riduzione del rischio informatico con un approccio che si pone dal punto di vista dell'attaccante

- Identificazione degli Asset in maniera autonoma, a partire da quanto esposto di un'organizzazione
- Spostare l'attenzione sul Rischio Analisi debolezze utilizzabili per exploit ed attacchi
- Guida specifica, prioritizzata, per la messa in sicurezza delle superfici a minor resistenza

Un sistema che evidenzia come gli **attaccanti*** vedono un'organizzazione e come ne identificano i punti più deboli da attaccare.
Pensare come un attaccante.

---

* Una volta solo gli attaccanti, oggi anche i partner

Caro Fornitore ti scrivo . . .

Gentile Fornitore,
la nostra Organizzazione utilizza **xxxxxx** *(https://www.xxxxxx.com) come strumento per il monitoraggio del* ***security rating****. Durante tale attività abbiamo rilevato un* ***peggioramento*** *del vostro* security rating.
Il security rating si basa sulle informazioni pubbliche presenti in rete relative alle vostre digital properties, ovvero asset digitali riconducibili alla vostra azienda (es. dominio), ed è composto da una serie di vettori legati alle principali vulnerabilità/esposizioni a rischi IT rilevabili tramite web.
*In particolare, sulla base delle attività di monitoraggio da noi svolte, vi segnaliamo un considerevole downgrade (****-50****) del vostro security rating, nel mese di Aprile.*
Nel dettaglio il vostro score è passato da nnn punti a ***mmm*** *[…].*
Di seguito riportiamo il dettaglio dei vettori di rischio che risultano oggetto di criticità e che hanno causato il relativo scostamento: […….]

Vi chiediamo di ***inoltrare*** *al vostro* ***referente per la Cybersecurity*** *tale comunicazione in modo tale che possa* ***intraprendere*** *al più presto* ***azioni di rimedio*** *volte a mitigare i rischi.*
Attendiamo conferma *dell'effettiva presa in carico della presente segnalazione e di* ***fornirci futuri aggiornamenti sullo stato avanzamento*** *delle attività di rimedio che avrete pianificato.*

Caro Partner ti rispondo . . . (male)

Buongiorno,

apprendiamo con un certo stupore che una ***società privata*** *come la vostra abbia affidato ad una* ***società straniera, extraeuropea,*** *il* ***monitoraggio sistematico*** *di tutti gli asset informatici di una* ***PA*** *e l'****individuazione*** *di tutte le sue vulnerabilità e la loro evoluzione nel tempo* ***senza****, a quanto risulta, alcun tipo di* ***autorizzazione, informazione o coinvolgimento del soggetto interessato****.*

Nell'accogliere la vostra disponibilità ad un confronto, si ritiene di svolgere queste prime considerazioni dal momento che pur comprendendo che risultando vostri fornitori cyber relevant, voi prestiate particolare attenzione al nostro Cybersecurity Mark, pur tuttavia risulta evidente che ***l'utilizzo indiscriminato****, senza il coinvolgimento dell'interessato, di uno* ***strumento scelto monolateralmente*** *su una public research university ad alta valenza tecnologica possa* ***dare risultati non così accurati*** *come potrebbe invece fare per una normale azienda e, soprattutto,* ***non risulta chiara l'autorizzazione all'analisi di indirizzi IP che costituiscono, come noto, dati personali.***

DORA, NIS2, D.Lgs. 90/24 & C.

Le recenti normative hanno introdotto, per coloro che si trovano all'interno di determinati «perimetri», l'obbligo di vigilare sul livello di sicurezza informatica dei propri fornitori «Cyber Critici».

Nel *Digital Operational Resilience Act* (DORA) viene introdotta l'**Accountability per i rischi ICT delle terze parti**.
Diviene obbligatorio occuparsi di **Supply Chain Risk Management** (SCRM).

Diviene fondamentale

- identificare gli asset più esposti e vulnerabili
- gestire il rischio informatico
- rispondere celermente
- potenziare la reattività degli «apparati di difesa» alle maggiori sollecitazioni

L’aspetto Organizzativo

Il crescere delle sollecitazioni sull’apparato di Cybersecurity rischia di rendere il tradizionale Modello Centralizzato di gestione del rischio (basato di fatto sul concetto di Shared Accountability) non più sostenibile.

- Vulnerability Assessment effettuato/esternalizzato centralmente
- Individuazione proprietari e amministratori asset a rischio
- Invio di report di segnalazione e richiesta remediation
- **Verifica** del lavoro effettuato
- Invio Sollecito
- Ri-verifica
- Ricomicia da capo (indipendentemente dall’esito dell’eventuale remediation)

si rivela assai dispendioso e produce scarsi risultati in termine di effettiva riduzione del rischio ed effetti sul Cybersecurity Mark

L’aspetto Organizzativo

Passare ad un modello di Distributed Accountability può dimostrarsi più efficace e rapido nei tempi di risoluzione, consentendo all’Unità di Cybersecurity centrale di operare con maggiore produttività.

- Attivazione di una rete di referenti informatici/incaricati cybersecurity nei vari centri, dipartimenti,…
- Gestione della superficie di attacco con la presa in carico dei propri asset, anche sotto il profilo della cyber-sicurezza, a livello di dipartimento, centro, . . .

L’aspetto Operativo

- Adozione di un sistema di Attack Surface Management
- Creazione sul sistema di raggruppamenti di asset da associare ai vari centri/dipartimenti
- Accesso di ogni operatore alla piattaforma con credenziali proprie e visione completa degli asset a lui/loro affidati, delle loro vulnerabilità e delle azioni da compiere per la riduzione del rischio, in ordine di gravità
- Unità di Cyber-sicurezza centrale con visione completa sugli asset funzioni di monitoraggio, supporto, coordinamento e formazione
- Importanza dei report
- Importanza della formazione e degli amministratori di sistema/operatori di cybersecurity

Caro Partner ti rispondo . . . (meglio)

Buonasera,

ringrazio per la cortese segnalazione *riguardo alle problematiche relative al security rating dell'ateneo.*
Abbiamo preso in carico *la vostra segnalazione ed effettuato una serie di analisi sui dati contenuti nell'excel che ci avete fornito e che per comodità ri-allego in risposta.*
Pur essendo tali ***segnalazioni*** *piuttosto* ***precise*** *e* ***circostanziate****,* ***ci preme comunque puntualizzarvi*** *[…]*
Ciò non toglie che il monitoraggio da voi effettuato abbia un'importante valenza e possa aiutarci a migliorare il livello complessivo di sicurezza della superficie esposta dell'ateneo.
Nello specifico, negli ultimi anni si è intrapresa l'adozione di uno specifico strumento per il monitoraggi della superficie di attacco esposta su internet. Saremmo lieti di condividere con voi l'andamento dei livelli di sicurezza delle risorse e dei servizi in rete.

Cogliamo l'occasione per comunicarvi che ci stiamo muovendo verso un ***modello di accountability distribuita in cui ogni dipartimento/struttura viene investita della responsabilità della gestione della sicurezza dei propri asset.*** *Lo strumento in uso consentirà un'analisi della sicurezza della singola struttura, permettendo quindi una verifica puntuale del livello di sicurezza della porzione di rete in cui viene effettuato e gestito uno specifico trattamento/processo.*

Alleghiamo in calce un'immagine dello stato degli asset e l'andamento negli ultimi mesi delle criticità più rilevanti da cui si può dedurre un lento ma costante miglioramento del livello complessivo di sicurezza.

Conclusioni

Distributed Accountability

(Ognuno sa di cosa è responsabile)

Shared Accountability

(tutti sono responsabili di tutto = nessuno è responsabile di niente)

Domande?

wooclap.com
Codice: WSGARR24

WORKSHOP GARR 2024

NET MAKERS

Thanks

www.linkedin.com/in/enricovenuto

Enrico Venuto

Politecnico di Torino

Politecnico di Torino