Sfide Digitali: Proteggiamo le Pubbliche Amministrazioni dagli attacchi informatici

Consapevolezza, la prima fase della sicurezza.

Cari Colleghi,

Come sapete, negli ultimi anni gli attacchi informatici e cibernetici ai danni delle Pubbliche Amministrazioni italiane sono in continuo sviluppo anche in virtù dell'aumento delle innovazioni tecnologiche.
A tal riguardo, appare necessario **contenere e combattere questi fenomeni** che quotidianamente ci troviamo a fronteggiare, in primis attraverso un incremento della **consapevolezza di tutti noi**.

Secondo i dati CLUSIT, la più importante associazione italiana per la sicurezza informatica, le **Pubbliche Amministrazioni risultano al primo posto** fra le realtà interessate da incidenti informatici.

La Regione Calabria ha riconosciuto **l'importanza della sicurezza informatica** e **della protezione dei dati personali**, soprattutto in un'epoca in cui le minacce informatiche sono sempre più sofisticate e frequenti. Per questo motivo, abbiamo deciso di avviare **una campagna che mira a informare e sensibilizzare** tutti noi sulla necessità di adottare comportamenti e strumenti adeguati per proteggere i nostri dati e le nostre informazioni. In particolare, la campagna si sostanzierà in **Newsletter trimestrali** che approfondiranno i temi della sicurezza informatica e della protezione dei dati personali, fornendo informazioni utili e **strumenti pratici** per una gestione efficace del tema. Dunque, l'obiettivo è promuovere una cultura basata sulla sicurezza.

Vi presentiamo, quindi, questa prima Newsletter al fine di illustrarvi i più recenti attacchi alle PA italiane, con lo scopo ultimo di aumentare **la consapevolezza** sul tema ed incrementare la tutela del nostro patrimonio informativo regionale.

Quali sono stati i principali attacchi alle PA italiane?

Maggio 2022: Un attacco DDoS (Distributed Denial of Service) è stato compiuto ai danni del Senato della Repubblica e del Ministero della Difesa Italiano. Responsabile dell'operazione era il collettivo russo "Killnet".

Marzo 2023: Un attacco Ransomware viene rivendicato dal gruppo criminale "RansomHouse" ai danni del Comune di Taggia. I dati esfiltrati sono stati interamente diffusi online e la quantità di file rubati durante l'attacco ammonta a 700 GB.

Maggio 2023: L'attacco è stato compiuto ai danni dell'ASL di Avezzano - Sulmona -L'Aquila, rivendicato dal gruppo criminale "Monti". I criminali riferiscono di aver esfiltrato grandi quantità di materiale sensibile di cittadini inerente al settore sanitario con un malware di tipo Ransomware.

Novembre 2023: L'Azienda Ospedaliera Universitaria Integrata di Verona ha subito un grave attacco. Si tratta, per la precisione, di una fuga di 658.828 file contenenti informazioni parziali e incomplete di utenti e collaboratori dell'Azienda ospedaliera, sia di natura sanitaria che amministrativa. L'attacco è stato rivendicato dal gruppo criminale "rhysida" che ha pubblicato i dati nel Dark Web.

Dicembre 2023: Westpole, azienda che fornisce servizi cloud alle Pubbliche Amministrazioni, è stata vittima di un attacco Ransomware del collettivo "Lockbit", che in passato ha rivendicato attacchi dello stesso tipo.

Gennaio 2024: Un accesso da parte di soggetti non autorizzati, attraverso un Ransomware, ha prodotto difficoltà all'interno del Sistema Sanitario della Regione Basilicata. Per gestire l'emergenza è stata allertata l'Unità di crisi dell'ACN (Agenzia per la Cybersicurezza Nazionale) che ha inviato i propri tecnici sul posto al fine di contenere l'attacco.

Febbraio 2024: Un attacco informatico di tipo Ransomware al sito web dell'Azienda Sanitaria Provinciale di Cosenza (ASP) ha generato problemi nell'erogazione di servizi essenziali. L'azione ha causato impedimenti all'accesso a vari servizi, tra cui prenotazioni, consultazioni online e ottenimento di informazioni riguardanti vaccinazioni e prestazioni sanitarie.

La sicurezza dei sistemi informatici è di **estrema importanza nel governo delle infrastrutture critiche** delle Pubbliche Amministrazioni locali, regionali e nazionali, data la gestione giornaliera di dati che interessano i criminali del web.
È stato notato come le associazioni criminali concentrino la loro attenzione ed i loro attacchi verso la sanità pubblica regionale. Di seguito le principali motivazioni:

La grande rilevanza che i dati personali detenuti da questi enti pubblici rivestono per la sicurezza pubblica: le Aziende Sanitarie Regionali hanno una probabilità molto più alta di effettuare **il pagamento di un riscatto** per la chiave di decodifica rispetto a qualsiasi altra azienda privata.

I benefici per chi commette l'attacco attraverso i disservizi che esso causa: rendere pubblico e conosciuto il nome del collettivo che ha compiuto l'attacco è di notevole interesse per i criminali, al fine di **guadagnare notorietà e credibilità** nella comunità dei criminali informatici (il cd. hacktivismo).

Il mero disservizio che si reca all'Amministrazione: la compromissione della **riservatezza, della disponibilità e dell'integrità dei dati personali** tipicamente discendente da questa tipologia di incidenti, si associa spesso anche al rischio di un concreto pregiudizio alla continuità dei servizi assistenziali.

In conclusione, il tema della sicurezza informatica è diventato negli ultimi tempi molto rilevante per le Pubbliche Amministrazioni, in quanto **i dati sensibili e le informazioni riservate** sono sempre più **esposti** a rischi di violazione e furto. Quindi, è fondamentale che le Amministrazioni si dotino di **strumenti e politiche di sicurezza adeguate** per proteggere il proprio patrimonio informativo e garantire la privacy dei cittadini. Nelle prossime Newsletter tali tematiche verranno approfondite con il fine di fornire ulteriori informazioni e strumenti utili a gestire efficacemente la sicurezza informatica e la tutela della riservatezza delle informazioni. In particolare, si incentreranno sui temi della **Privacy** e della **tutela del nostro patrimonio informativo**.

Saluti,
Settore "Infrastrutture Digitali e Sicurezza",
Responsabile Protezione Dati,
Ufficio Privacy Regione Calabria.