Clusit: cyber war, Italia già esposta a nuovi rischi; necessario innalzare la soglia di allerta

L'Associazione Italiana per la Sicurezza Informatica raccomanda che istituzioni ed imprese seguano le indicazioni CSIRT nazionale ed evidenzia quattro punti chiave per la difesa:

1. **Non sottovalutare anomalie nei sistemi informativi**
2. **Diligenza verso le policy aziendali**
3. **Verifica costante dell'efficacia delle misure di sicurezza in atto**
4. **Attenzione a monitoraggio early warning e threat intelligence**

Milano, 2 marzo 2022 – La situazione geopolitica espone in questi giorni i sistemi informativi delle organizzazioni a rischi che, se non nuovi, sono sicuramente di portata maggiore. "*L'evoluzione dello scenario è particolarmente rapida e una ulteriore escalation consisterà inevitabilmente di azioni efficaci in tempi fulminei. È importante che la reazione a possibili attacchi sia tempestiva e coordinata*", afferma Claudio Telmon, membro del comitato direttivo Clusit, l'Associazione Italiana per la Sicurezza Informatica.

Clusit raccomanda in primo luogo ad imprese istituzioni italiane di seguire con attenzione le comunicazioni e le indicazioni che vengono tempestivamente fornite dal **CSIRT nazionale**, il Computer Security Incident Response Team italiano, attivo nel fornire indicazioni di scenario e su minacce e vulnerabilità specifiche. Grazie al continuo coordinamento con attori a livello europeo ed internazionale, il nostro Computer Security Incident Response Team dispone infatti di informazioni tempestive a cui altre fonti potrebbero non avere accesso.

Quattro sono poi i punti fondamentali su cui l'Associazione Italiana per la Sicurezza Informatica esorta la massima allerta:

1. Aumentare il **livello di attenzione a possibili anomalie** che possano essere indicative di attacchi in corso. "*Questa indicazione non riguarda solo le aziende che abbiano rapporti con l'Ucraina o la Russia ma, indistintamente, tutte le organizzazioni; infatti, nel momento in cui l'evoluzione dello scenario portasse l'Italia ad essere più direttamente oggetto di attacco, gli eventi si potrebbero sviluppare molto rapidamente*", precisa Telmon.

2. Cogliere l'occasione per ricordare al proprio personale le **politiche aziendali in termini di sicurezza delle informazioni**, rinnovando in particolare l'attenzione alle regole di comportamento per evitare di essere oggetto di attacchi di phishing o veicolo di attacchi da parte di malware.

3. Verificare l'**efficacia delle proprie misure di sicurezza**, comprese quelle per assicurare la disponibilità di servizi e informazioni anche in caso di attacchi importanti ai propri sistemi; in particolare, verificare almeno la disponibilità e la correttezza di backup aggiornati e offline e, dove presenti, l'efficacia dei processi e meccanismi di **disaster recovery**.

4. Assicurare che **servizi di early warning e threat intelligence** eventualmente acquisiti come servizio siano attivi, funzionanti e, da non sottovalutare, che siano monitorati.

###

Clusit è l'Associazione Italiana per la Sicurezza Informatica. Nata nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, rappresenta oggi oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese. Clusit collabora con la Presidenza del Consiglio, con diversi Ministeri, Authority, Istituzioni e organismi di controllo, tra cui Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali. Svolge inoltre un'intensa attività di supporto e di scambio con le Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA, con Università e Centri di Ricerca. In ambito internazionale, Clusit partecipa a diverse iniziative in collaborazione con i CERT, i CLUSI, con la Commissione Europea, ENISA (European Union Agency for Cybersecurity), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), con le principali Associazioni Professionali del settore, con Università e Centri di Ricerca in oltre 20 paesi. Ulteriori informazioni sulle attività di Clusit sono disponibili sul sito www.clusit.it.

Per ulteriori informazioni si prega di contattare:

Daniela Sarti
Ufficio Stampa Security Summit | Clusit
press@securitysummit.it - dsarti@clusit.it
Tel. 335 459432