

venerdì 10 dicembre 2010, ore 12.10

Segnali stradali a rischio hacker



La segnaletica luminosa a pannelli variabili nel mirino di un virus che potrebbe modificare i messaggi agli automobilisti

red

Allarme sicurezza per i segnali stradali a pannelli variabili: gli hacker possono penetrare impunemente nel sistema modificando a proprio piacimento i testi dei messaggi stessi. Non solo: sono a rischio anche le dilaganti connessioni tra smartphone e automobili, grazie alle quali potrebbero trasmettersi virus informatici in grado di bloccare o modificare le centraline elettroniche delle auto. Questa la denuncia della Fondazione Icsa che ha anche ricordato come un virus particolarmente pericoloso, il rootkit Stuxnet, abbia mandato in tilt migliaia di sistemi di controllo legati alla gestione delle infrastrutture. "Le reti che gestiscono le infrastrutture dei sistemi di trasporto - ha spiegato Marcello Pistilli, business development manager Information Security Eustema - sono destinate a convergere verso il mondo del web, complice la pervasività di Internet e la grande diffusione di strumenti che facilitano il contatto con gli utenti sempre e ovunque (mediante hot spot Wi-Fi ad accesso libero, servizi di Internet mobile o di geolocalizzazione)". Secondo le principali istituzioni impegnate nella lotta al cyber crimine, le infrastrutture che sovrintendono alla mobilità di centinaia di milioni di persone in tutto il mondo sono già attentamente monitorate da gruppi internazionali organizzati con finalità criminali. Questo trend obbliga ad una seria riflessione su come far fronte alle vulnerabilità già riscontrate e su come attrezzarsi al meglio per salvaguardare tali asset strategici nel prossimo futuro. Si è verificato che la definizione e verifica delle procedure chiamate a governare l'infrastruttura della sicurezza (dal punto di vista fisico e logico) non può prescindere da interventi sul reale anello debole della catena: il fattore umano. A tal proposito è opportuno sottolineare che Stuxnet, il pericolosissimo virus che lo scorso luglio ha messo in ginocchio decine di migliaia di sistemi di controllo Scada, non è stato veicolato tramite web ma diffuso consapevolmente da un individuo mediante una chiavetta USB. Per questa ragione è necessario affiancare ai tradizionali servizi di risk analysis, solution design and implementation, physical & logical security, incident & threat management, specifiche modalità di assesment e

collaudati percorsi di formazione che garantiscono un'interoperabilità consapevole e priva di rischi tra le persone prima ancora che tra i differenti strumenti informatici". Insomma il rischio c'è ed è anche concreto tant'è che nel corso del convegno della Fondazione Icsa il Comitato di Coordinamento interministeriale per la sicurezza dei Trasporti e delle Infrastrutture, ha annunciato che è pronto un provvedimento per la sicurezza delle infrastrutture critiche e la loro protezione che dovrebbe essere presentato in Consiglio dei Ministri.