ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5131 di Lunedì 28 marzo 2022

La guerra in Ucraina e i riflessi sulla sicurezza informatica

Il concetto di guerra e armi utilizzate deve essere interpretato in maniera più allargato rispetto al passato. La componente informatica, infatti, può rappresentare un aspetto significativo degli strumenti di attacco che un paese in guerra può utilizzare.

Numerose autorità pubbliche, coinvolte nella sicurezza dei sistemi informativi e, di riflesso, della protezione dei dati personali, si sono recentemente allertate, a seguito della invasione della Ucraina da parte della Russia.

Come era d'altronde prevedibile, ad azioni di guerra di tipo tradizionale si stanno associando anche azioni di guerra di tipo non tradizionale, come ad esempio attacchi informatici. In questo contesto è sensibilmente cresciuta la attenzione posta all'utilizzo di applicativi, provenienti da vari paesi del mondo, ed utilizzati addirittura per mettere in sicurezza i nostri sistemi informativi.

Un problema analogo, che certamente i lettori ricorderanno, si pose alcuni anni fa, quando una delle maggiori aziende produttrici di telecamere del mondo, con base in Cina, vide i propri prodotti messi sotto la lente di ingrandimento informatica di organismi specializzati statunitensi. Questi organismi giunsero alla conclusione che era possibile che nel software di gestione di queste telecamere potessero essere inserite funzionalità nascoste di vario tipo.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0836] ?#>

Tornando ai tempi presenti, la neonata agenzia per la cybersicurezza nazionale ha lanciato un messaggio di allarme a tutte le pubbliche amministrazioni, che utilizzano applicativi antivirus e, più in generale, applicativi di sicurezza informatica, aventi origine da uno dei maggiori produttori russi.

Questa allerta è stata inviata non tanto sulla base di una oggettiva rilevazione di possibili debolezze di questi software di protezione, ma nel quadro di un legittimo sospetto, circa appunto la possibile presenza di queste debolezze.

Giova infatti sottolineare, ad oggi, che gli organismi incaricati di tutelare la sicurezza dei sistemi informativi nazionali non hanno documentato od identificato debolezze specifiche; si tratta quindi di un atteggiamento cautelativo, d'altronde del tutto comprensibile in un mondo in così veloce evoluzione, come quello della sicurezza informatica.

Sulla stessa linea si è recente mossa anche la nostra autorità garante per la protezione dati personali, che forse anche sulla base del messaggio di allarme inviato dalla agenzia per la cybersecurity nazionale, ha chiesto al produttore di questi applicativi di fornire tutt'una serie di informazioni sulle modalità con cui i dati personali, che si trovano all'interno di sistemi informativi protetti da questi applicativi antivirus, potrebbero o meno essere esposti a possibilità di comunicazione non autorizzata a soggetti terzi o addirittura di cancellazione.

Un dubbio legittimo, chiaramente evidenziato dall'avvio dell'istruttoria dell'autorità garante, fa proprio riferimento al fatto che sia possibile, nel corso del trattamento di dati, mediante sistemi protetti da questi applicativi antivirus, che i dati presenti nei sistemi di trattamento siano trasferiti al di fuori dell'unione europea, ad esempio nella federazione russa.

A questo tema non sono solo interessate l'autorità di tutela della nostra nazione, ma anche le autorità di tutela di altre nazioni, tant'è vero che la nostra autorità garante ha chiesto esplicitamente di conoscere quante altre autorità governative di paesi terzi, a partire dal 1° gennaio 2021, hanno avanzato richieste o attivato istruttorie, simili a quelle attivate dalla nostra autorità nazionale.

Sulla base di queste informazioni, credo che sia opportuno che i nostri lettori, che utilizzano questi applicativi, effettuino una valutazione aggiornata e approfondita circa l'utilizzo di tali applicativi.

Adalberto Biasiotti

Licenza Creative Commons

www.puntosicuro.it