□□ Cybersecurity nel retail: il governo UK risponde agli attacchi a Harrods e M&S

Maria Cattini | 04/06/2025 | Sicurezza digitale

In arrivo un piano da 16 milioni di sterline per difendere aziende, cittadini e democrazie digitali

□□ Il contesto: una settimana nera per la moda britannica

Nelle ultime settimane, **Marks & Spencer, Harrods e la Co-op** sono state colpite da attacchi informatici su larga scala, costringendo le aziende a sospendere ordini online, bloccare i sistemi di pagamento e interrompere processi interni.

Il caso M&S ha avuto un forte impatto mediatico: un ransomware ha compromesso interi servizi, costringendo l'azienda a chiudere alcune operazioni digitali e a posticipare nuove assunzioni.

□□ La risposta del governo: non più un optional

Il ministro Pat McFadden ha definito la questione con parole dure durante la conferenza CyberUK di Manchester:

> "Gli attacchi informatici non sono un gioco. Sono criminalità organizzata. Una forma moderna di estorsione.

E per affrontarla, è stato presentato un pacchetto di **16 milioni di sterline**, articolato su più fronti.

□□ Le novità in arrivo

1. CHERI, il chip che blocca il 70% degli attacchi comuni

Tra le misure chiave, il finanziamento per lo sviluppo della tecnologia **CHERI**, un microchip con protezioni avanzate che potrebbe fermare gran parte degli attacchi informatici più diffusi.
□□ Previsti **4,5 milioni di sterline** per accelerarne l'arrivo sul mercato.

2. Un codice di sicurezza per chi sviluppa software

Il governo pubblicherà un **"software security code of practice"**, con linee guida essenziali per tutte le aziende che creano o vendono software nel Regno Unito.

3. Sostegno all'AI e alla difesa digitale internazionale

- 7 milioni per il Laboratorio britannico per la sicurezza dell'intelligenza artificiale.
- 8 milioni per il programma di difesa cyber dell'Ucraina.

• Oltre 1 milione per proteggere l’integrità delle elezioni in Moldova.

□□ Una visione strategica: la cybersecurity come industria chiave

Il piano non è solo difensivo. Il governo UK vuole fare della **cybersecurity una leva di crescita industriale**:

> “Con oltre 2.000 aziende attive nel Regno Unito, il settore può diventare motore di nuovi posti di lavoro, innovazione e leadership globale.

McFadden ha annunciato che la difesa digitale sarà uno dei pilastri della prossima **strategia industriale nazionale**.

□□Perché riguarda anche la moda**?**

Il settore retail è uno dei più esposti, perché:

• gestisce grandi quantità di dati personali (clienti, transazioni, carte di pagamento),
• dipende da sistemi IT altamente interconnessi,
• ha ritmi serrati e vulnerabilità logistiche.

Gli attacchi a M&S e Harrods dimostrano che **nessun brand, per quanto prestigioso, è immune**.

□□ La sicurezza è la nuova reputazione

Per i brand della moda e del retail, la cybersecurity oggi non è più solo un tema tecnico.
È una **scelta strategica** che tocca fiducia, continuità operativa e reputazione.
E ora è chiaro: **chi non investe in sicurezza, investe nel rischio**.

In arrivo un piano da 16 milioni di sterline per difendere aziende, cittadini e democrazie digitali

□□ Il contesto: una settimana nera per la moda britannica

Nelle ultime settimane, **Marks & Spencer, Harrods e la Co-op** sono state colpite da attacchi informatici su larga scala, costringendo le aziende a sospendere ordini online, bloccare i sistemi di pagamento e interrompere processi interni.

Il caso M&S ha avuto un forte impatto mediatico: un ransomware ha compromesso interi servizi, costringendo l’azienda a chiudere alcune operazioni digitali e a posticipare nuove assunzioni.

□□ La risposta del governo: non più un optional

Il ministro Pat McFadden ha definito la questione con parole dure durante la conferenza CyberUK di Manchester:

> “Gli attacchi informatici non sono un gioco. Sono criminalità organizzata. Una forma moderna di estorsione.

E per affrontarla, è stato presentato un pacchetto di **16 milioni di sterline**, articolato su più fronti.

□□ Le novità in arrivo

1. CHERI, il chip che blocca il 70% degli attacchi comuni

Tra le misure chiave, il finanziamento per lo sviluppo della tecnologia **CHERI**, un microchip con protezioni avanzate che potrebbe fermare gran parte degli attacchi informatici più diffusi.
□□ Previsti **4,5 milioni di sterline** per accelerarne l'arrivo sul mercato.

2. Un codice di sicurezza per chi sviluppa software

Il governo pubblicherà un **"software security code of practice"**, con linee guida essenziali per tutte le aziende che creano o vendono software nel Regno Unito.

3. Sostegno all'AI e alla difesa digitale internazionale

• 7 milioni per il Laboratorio britannico per la sicurezza dell'intelligenza artificiale.
• 8 milioni per il programma di difesa cyber dell'Ucraina.
• Oltre 1 milione per proteggere l'integrità delle elezioni in Moldova.

□□ Una visione strategica: la cybersecurity come industria chiave

Il piano non è solo difensivo. Il governo UK vuole fare della **cybersecurity una leva di crescita industriale**:

> "Con oltre 2.000 aziende attive nel Regno Unito, il settore può diventare motore di nuovi posti di lavoro, innovazione e leadership globale.

McFadden ha annunciato che la difesa digitale sarà uno dei pilastri della prossima **strategia industriale nazionale**.

□□Perché riguarda anche la moda**?**

Il settore retail è uno dei più esposti, perché:

• gestisce grandi quantità di dati personali (clienti, transazioni, carte di pagamento),
• dipende da sistemi IT altamente interconnessi,
• ha ritmi serrati e vulnerabilità logistiche.

Gli attacchi a M&S e Harrods dimostrano che **nessun brand, per quanto prestigioso, è immune**.

□□ La sicurezza è la nuova reputazione

Per i brand della moda e del retail, la cybersecurity oggi non è più solo un tema tecnico.
È una **scelta strategica** che tocca fiducia, continuità operativa e reputazione.
E ora è chiaro: **chi non investe in sicurezza, investe nel rischio**.