	> Avanzate > Privacy e sicurezza > Impostazioni sito > Microfono e impostare su "Chiedi prima di accedere (opzione consigliata)".

Hardening del browser: MIME Sniffing	
Minaccia	- Attacchi all'integrità dei sistemi. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	Abilitare la barra delle informazioni per consentire all'utente di visualizzare il risultato di un'azione (es. cliccare su un link) prima di effettuarla. Disabilitare la possibilità per i siti web di iniziare un download senza l'accettazione esplicita dell'utente, ad es. da codice (Internet Explorer). Abilitare le funzionalità di MIME Sniffing che consentono di "marcare" un file collegato a un download attraverso il suo MIME Type, per evitare che un codice eseguibile venga visualizzato come testo o altro documento (es. PDF) per invogliare l'utente ad aprirlo.

Hardening del browser: segnalazione errori	
Minaccia	Divulgazione di informazioni riservate.
Contromisure	Limitare/Disabilitare i servizi di "segnalazione automatica degli errori", al fine di evitare la divulgazione di dati personali e di altre informazioni riservate.

Hardening del sistema operativo che ospita il browser	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Eseguire l'hardening del sistema operativo che ospita il browser. L'hardening del sistema operativo è oggetto di un paragrafo specifico [rif. 5.2.2]

5.3.3 Autorizzazione

Ai principi generali introdotti nel paragrafo [rif.5.1.3], si aggiungono le indicazioni, di cui di seguito:

Autorizzazione	
Minaccia	Accesso non autorizzato al sistema (macchina, configurazione, etc.)
Contromisure	Proteggere i parametri di sicurezza dagli utenti finali: essi devono essere modificabili solo da un'utenza amministrativa.

5.3.4 Crittografia

Ai principi generali introdotti nel paragrafo [rif. 5.1.4], si aggiungono le indicazioni, di cui di seguito:

Crittografia	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Crittografia debole o non validata. - Generazione e/o gestione inadeguata delle chiavi crittografiche.
Contromisure	Valgono i principi generali introdotti nel paragrafo [rif. 5.1.4].