IIS Extended Protection

X msxfaq.de/windows/iis/iis_extended_protection.htm

Frank Carius

With Exchange 2019 CU14, many administrators startled because the "Extended Protection" function must be activated. However, the function is part of the IIS since Windows 2012R2 and is only used by Microsoft as text described. I wanted to know what Extended Protection and how it is not only Exchange but also other services.

Please also note CVE-2024-21410 consideration and Exchange Extended Protection and Extended Protection with internal Certificates

Note: Extended Protection was added in March 2010 as an update with Windows Server 2003 already provided.

The topic not only affects web servers, but is also related to LDAP (see LdapEnforceChannelBinding) and other protocols that need to be better secured against MITM attacks.

What is it about?

When a client accesses protected data on a server then he has to log in and as well as data transmission, such Connections can be encrypted and signed via TLS. Now but an attacker can trick the client into using the credentials through it as an intermediary. The User does not always notice this and the actual server sees only a legitimate connection of the attacker. The fact that the TLS connection is not continuous, neither can see. Extended Protection achieves the compatible registration procedures with information from the certificate. Since the attacker hopefully no access to the private key of the web server the attacker stands out in the communication that Login is not possible and the attacker does not receive a Credentials.

"Extended Protection" is an additional protection that only for TLS connections with the "Windows integrated Login (WIA)" and is enforced by the web server . However, "Extended Protection" has been available since 2010 the default has never been activated or enforced, as the Clients must support this.

Function Matrix

You can set "Extended Protection" on the IIS, which further down the page. For the function, we have to look at three components:

- IIS/Webserver
  Here you can use "Extended Protection" per virtual directory to one of the values Set "None", Accept, Require"
- Proxy/ReverseProxy/Load Balancer
  Here you can only choose between "Same" or "unequal" certificate
- Client
  The client can also use Extended Protection either not, only optional, or forced support.

Accordingly, the following table results:

IIS Setting	Certificate	Client	Registration	Description
None	Unequal	No	Yes	No one forces XP, so registration is possible
None	Unequal	Optional	Yes	No one forces XP, so registration is possible
None	Unequal	Require	No	The client only allows EP but if it's the server can't, no Registration
Accept	Unequal	No	Yes	No one forces XP, so registration is possible
Accept	Unequal	Optional	No!	At have it optional and therefore try to get EP, which but due to the Different certificates. A fallback to a Registration without EP can be found does not normally take place
Accept	Unequal	Require	No	The client enforces EP and the server offers it but due to the Different Certificates succeed not. A fallback to a Registration without EP can be found does not normally take place
Require	Unequal	No	No	However, the server forces the client can't do EP. Then the certificate is also no longer important

Require	Unequal	Optional	No	The server enforces and the client tries to get EP but due to the Different Certificates succeed not. A fallback to a Registration without EP can be found does not normally take place
Require	Unequal	Require	No	Due to the Different Certificates succeed not. A fallback to a Registration without EP can be found does not normally take place
None	Identical	No	Yes	Registration is open but not secured by EP
None	Identical	Optional	Yes	Registration is open but not secured by EP
None	Identical	Require	No	If the client EP but the server forces it can't, there is no Registration is complete
Accept	Identical	No	Yes	Registration is open but not secured by EP
Accept	Identical	Optional	Yes	Registration is open and secured by EP
Accept	Identical	Require	Yes	Registration is open and secured by EP
Reqire	Identical	No	No	Registration is not possible
Require	Identical	Optional	Yes	Registration is open and secured by EP
Require	Identical	Require	Yes	Registration is open and secured by EP

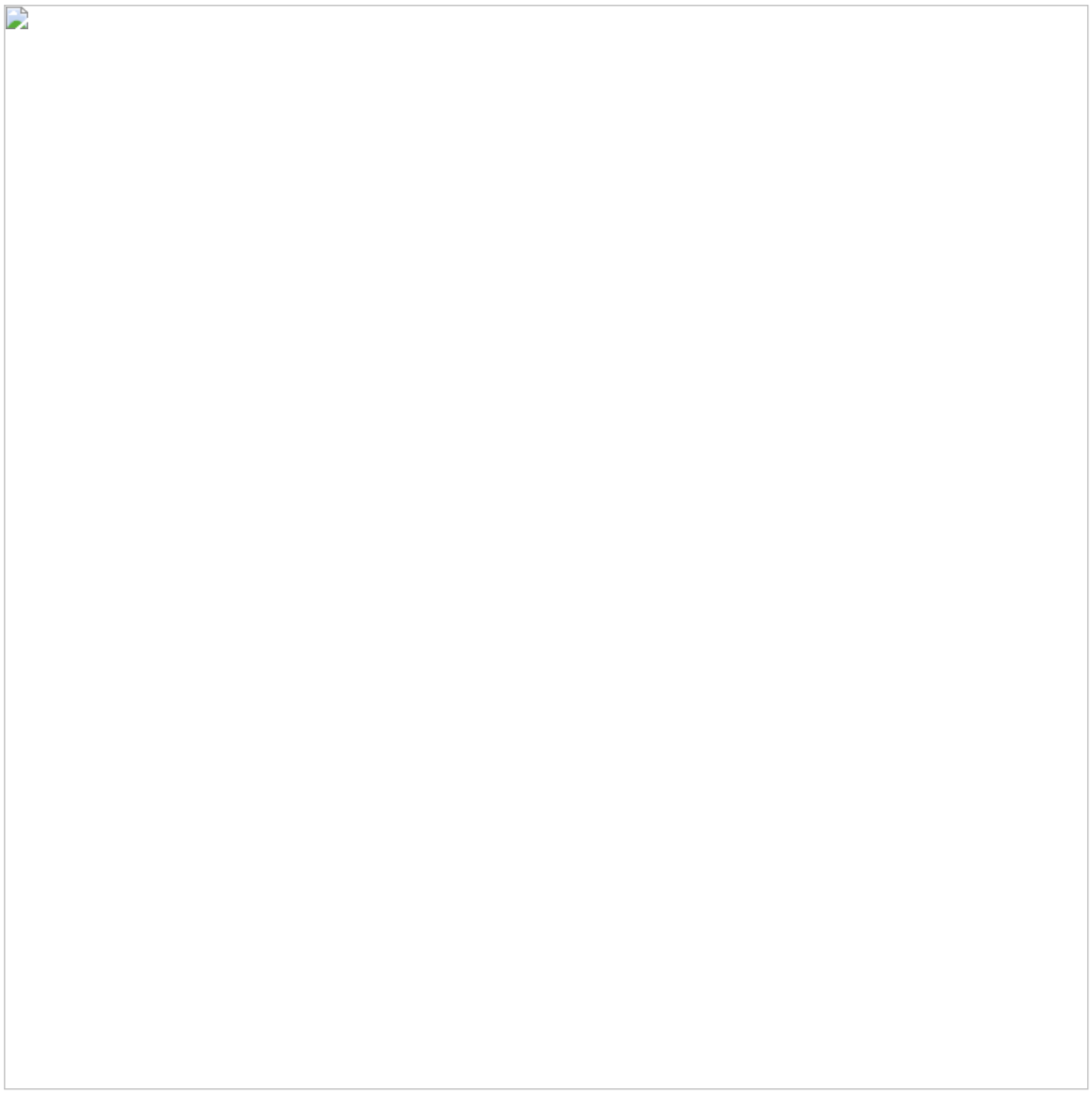
The MRS service in Exchange Online is an HTTP client that that does not enforce "Extended Protection" but uses it if it is offered. I have the corresponding lines in "yellow" marked. This means that there are only a few functioning Combinations:

- If a different certificate is used, then your Exchange Server set
  to NONE All other settings work not!
- With the same certificate, you can
  because MRS is set to "optional" and therefore he can register by EP if the certificates, but if the Exchange does not offer XP, then it reports via NTLM even without XP

So there are always problems when you are on the Exchange Server set the Extend Protection feature to Require but only set it to "Accept", because Exchange Online then do not log in to different certificates can.

TLS alone is not secure

A communication between a client and a server should always be encrypted, signed and encrypted when accessing private data must also be authenticated.



The TCP connection secures the transmission against lost packets and restores the correct order sure. On the one hand, the TLS connection ensures a Encryption of the data, however, is allowed by the certificate "Zert1" also tells the client to change the identity of the server. because the addressed URL is also included in the certificate must be included. Of course, it is no protection if an attacker is already foisting a "similar" domain.

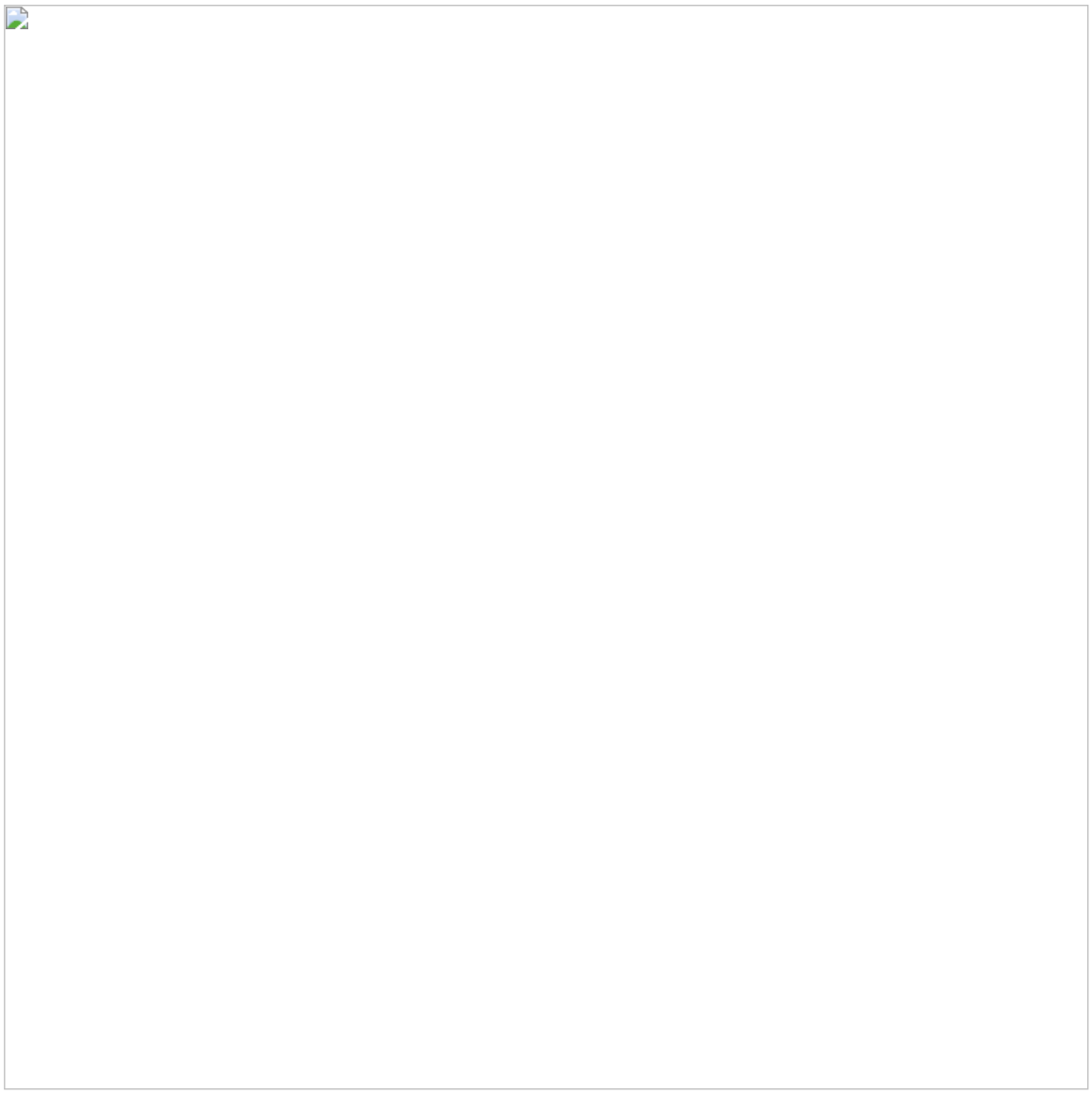
The TLS handshake works in such a way that the client sends a TLS hello with the possible encryption methods and the server selects the safest possible and the answer also includes its certificate with the public key transfers. This allows the client to be connected to a channel binding token, which only the server with the appropriate private key. Thus, both endpoints have a common key for faster and cheaper Symmetric encryption of data.

Via the secure channel I can now even use insecure Login procedures such as "BasicAuth", "bearer tokens" or Transfer form data and don't have to worry about it that the registration is carried out via "secure" procedures such as e.g. NTLM or Kerberos. These procedures are also work again with Channel Binding Token (CBT) to avoid passwords. transmit.

This supposed security becomes problematic when You break the TLS connection on the transmission path. There are legitimate and non-legitimate reasons for this.

Breaking TLS: Proxy

Companies want or need to transfer data for attacks, malware, or targets. But since most websites are now accessible via TLS, firewalls can on the cable only the encrypted See connections. Starting with TLS 1.3, a filter solution no longer even the server name in the "Client Hello" examine. Therefore, companies use proxy servers in their own network or in the cloud (Zscaler, Umbrella, etc.). That works because here the administrator has control over the client and gives it both the proxy via a configuration (Group Policy or WPAD), as well as its own certificate authority as "Trusted" .



The client connects securely via TCP or TLS to the Proxy Server and then starts a "CONNECT Target Server" However, the proxy does not direct access directly to the destination, but generates a certificate for the target via its own PKI, that is trusted by the client. The TLS connection is broken at the proxy server and the Server can see, check and, if necessary, change the transmitted data. block.

What is legitimate in companies can of course also be a Developers with tools like Fiddler on your computer for analysis. It becomes criminal when of the user on a "free" PC, e.g. in a hotel or Internet Café and the operator uses the same system to espionage. Then he can also "see" what the and insecurely transmitted passwords (BasicAuth, forms, NTLM hash values, bearer tokens). Such Systems are not difficult to set up. Therefore, there has been e.g. DANE - DNS-Based Authentication of Named Entities, which allows providers to Publish certificates of their web servers. So you can Browser may report an unexpected new certificate. However, this does not help on foreign computers.

This is where Extended Protection or MTLS protects

- SSL Inspection
- Fiddler
- DANE - DNS-Based Authentication of Named Entities
- HTTP Proxy Authentication
- Configure Fiddler Classic to Authenticate to CBT-Protected Server
  https://docs.telerik.com/fiddler/configure-fiddler/tasks/authenticatewithcbt
- Cain & Abel
  https://de.wikipedia.org/wiki/Cain_%26_Abel

Breaking TLS: ReverseProxy

Also on the other side in front of the web server there is a need for the To break connections. Several reasons can be listed here

- DoS protection, filtering
  , so-called "web application firewalls" take advantage of the good and evil combinations to the Internet and schedule the TLS channel. The incoming HTTP requests of the Clients are supported on these systems pre-filtered. The reverse proxy can, for example: see the URL in plain text and see the allowed Exchange Server Paths (/OWA, /EWS, /Microsoft-Server-ActiveSync, /OAB) known. Other accesses to /ECP or /PowerShell and traversal attacks on ".. /.. /.. /.. /Windows/cmd.exe" can be used directly blocked.
- Portal/PreAuthentication
  The client can also be used directly with a Login dialog for authentication . Many companies publish their servers via a portal, where the user can use a strong authentication before he then click on the various published applications. It works very good with interactive accesses but not so well with e.g. ActiveSync or MAPI/HTTP or the accessibility of Exchange for a hybrid deployment (MRSProxy migration, Free/Busy Times
- Load balancing/availability according to User/Session
  The last aspect is the distribution of the Access to multiple servers via one Load balancer. Of course, this can be done on Layer-4 (TCP) per connection. The Load balancer could also help the user "know" and control all his accesses via various parallel connections to the same server. If he does this with TLS (Layer-7), he can also use other Header (X-Forwarded-For) so that the backend server can use this .

In all three cases, the TLS connection is broken:

Übrigens gilt dies auch für Reverse Proxy in der Cloud wie den Azure AD Application Proxy

Jegliches Aufbrechen reduziert aber die Sicherheit der übertragenen Daten, da Sie ja nicht wissen, wer da mitliest.

Der Einsatz von Extended Protection mit der Prüfung der Channel Binding Tokens erfordert natürlich den Einsatz von TLS. Unterschlüsselte Verbindungen sollten Sie daher generell nicht mehr erlauben, wenn eine Authentifizierung erfolgt.

- SSL-Inspection
- X-Forwarded-For

- HTTPS Token Binding with TLS Terminating Reverse Proxies draft-ietf-tokbind-ttrp-09 https://datatracker.ietf.org/doc/html/draft-ietf-tokbind-ttrp

So schützt Extended Protection

Sowohl beim TLS-Handshake als auch bei der Anmeldung werden Channel Binding Token (CBT) verwendet, die bislang aber nicht miteinander verknüpft waren. Wenn Extended Protection aktiviert wird, dann erzwingt der Webserver die Kopplung der beiden Schlüssel. Sowohl beim Aufbrechen der Verbindung durch einen ausgehenden Proxy als auch durch einen eingehenden Loadbalancer oder Reverse Proxy wird aber die TLS-Verbindung aufgebrochen.

Da jede TLS-Verbindung seinen eigenen Channel Binding Token zum Verschlüssel verwendet und dieser sogar während der Verbindung geändert werden kann, nutzen der Client als auch der Webserver in diesem Fall unterschiedliche Channel Binding Tokens (CBT). Wenn die Authentifizierung nun ebenfalls Channel Binding Token mit prüfen, fällt der Bruch direkt auf.

Extended protection enhances the existing Windows Authentication functionality to mitigate authentication relay or "man in the middle" attacks. This mitigation is accomplished by using security information that is implemented through two security mechanisms:
1. Channel binding information that is specified through a Channel Binding Token (CBT). This is used primarily for SSL connections.
2. Service binding information that is specified through a service principal name (SPN). This is used primarily for connections that do not use SSL or when a connection is established. For example, this might be in a scenario in which SSL is offloaded to another device, such as a proxy server or load-balancer.
Quelle: Description of the update that implements Extended Protection for Authentication in Internet Information Services (IIS) - Microsoft Support

Extended Protection wirkt bei verschlüsselten Verbindungen über das Channel Binding Token während bei unverschlüsselten Verbindungen der SPN genutzt wird. Da mittlerweile wohl die meisten Verbindungen per TLS verschlüsselt sind, beschränke ich mich bei der weiteren Beschreibung darauf

...Currently, when a client application authenticates itself to the server using Kerberos, Digest, or NTLM using HTTPS, a Transport Level Security (TLS) channel is first established and authentication takes place using this channel. However, there is no binding between the session key generated by Secure Sockets Layer (SSL) and the session key that is generated during authentication. ..

...The solution is to use a TLS-secured outer channel and a client-authenticated inner channel, and to pass a Channel Binding Token (CBT) to the server. The CBT is a property of the TLS-secured outer channel, and is used to bind the outer channel to a conversation over the client-authenticated inner channel. ...
Quelle: Extended Protection for Authentication Overview https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/extended-protection-for-authentication-overview
Der Abschnitt sagt aber indirekt auch, dass eine Anmeldung per BasicAuth, Formulare oder OAUTH-Tokens nicht mit Channel Binding Tokens abgesichert werden.

Das dürfte auch der Grund sein, warum ich einen per Extended Protection gesicherten Exchange 2019 Server über einen Azure AD Application Proxy weiter erreichen kann.

Umgekehrt dürfte eine Anmeldung per Client Zertifikat, Smartcard und damit auch Windows Hello auch ohne Extended Protection als sicher gelten, da hier auch der Client seinen privaten Key nutzt, den weder der ausgehende noch ein eingehender Proxy hat. EP kann aber nur funktionieren, wenn die Verbindung auch per TLS verschlüsselt ist. Sie sollten also einen unverschlüsselten Zugriff direkt unterbinden (Port 80 sperren) oder über einen Redirect umleiten.

Das spiegelt sich auch bei der Aktivierung von EP auf Exchange wieder, wo SSL Offloading erst abgeschaltet werden muss.

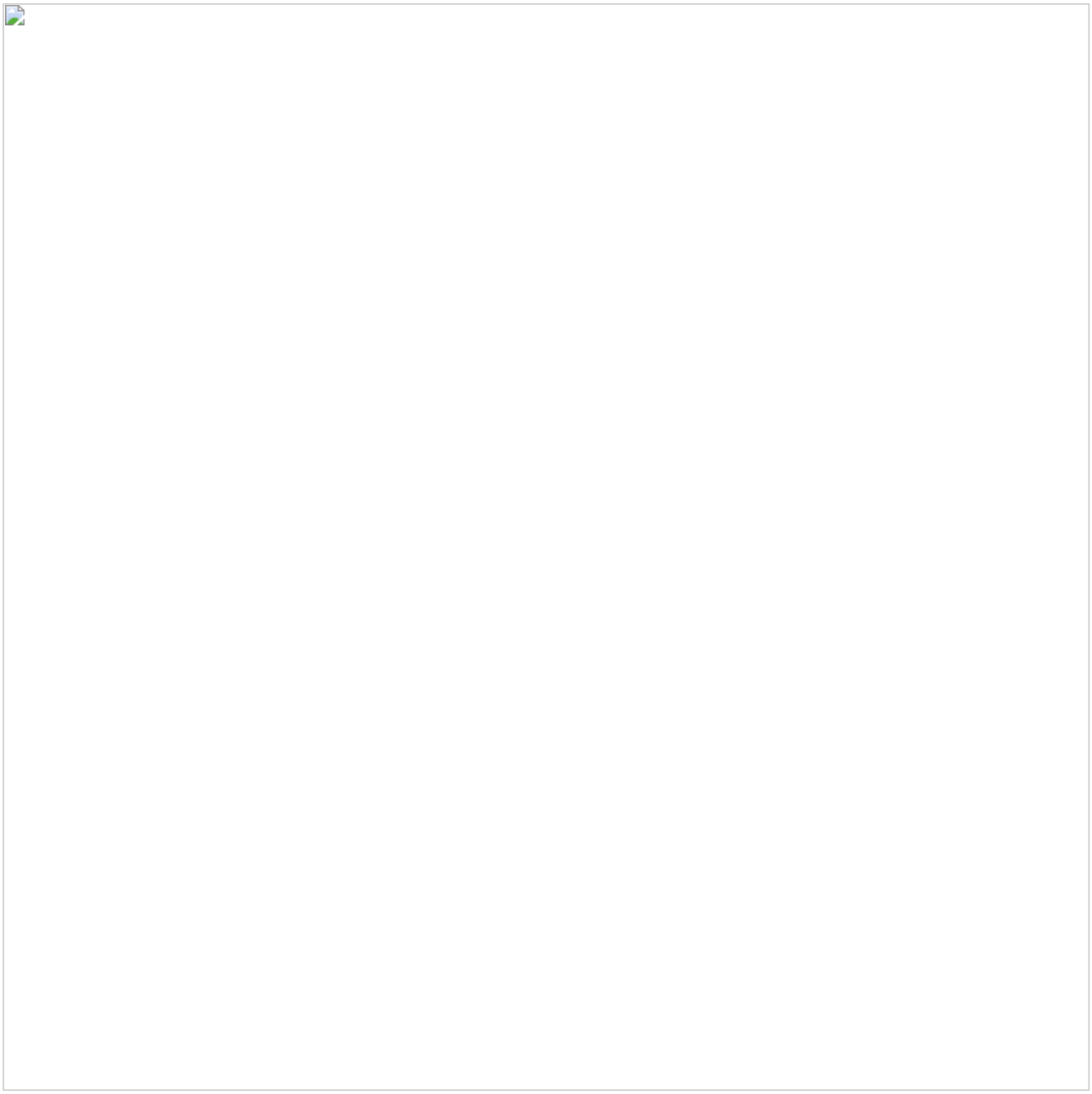
- Extended Protection for Authentication Overview https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/extended-protection-for-authentication-overview
- Configure Windows Extended Protection in Exchange Server https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/extended-protection-for-authentication-overview
- HTTP Authentication
- Authentifizierung im Wandel der Zeit
- SSL-Inspection
- Bearer Decoding

EP und Abhängigkeiten

Sie wissen nun, wie EP eine Anmeldung über eine TLS-Verbindung und Anmeldung mit der Kopplung von Channel Binding Tokens besser absichert. Der Einsatz von Extended Protection ist erforderlich, wenn Sie gegen Angriffe bezüglich CVE-2024-21410 abgesichert sein wollen. Dies vorgebliche Lücke liegt nämlich nicht im Exchange Code und kann daher dort auch nicht korrigiert werden, sondern in einer unsicheren Anmeldung mit Replay-Attacken durch NTLM-Tokens.

Ehe Sie aber nun Exchange Extended Protection einsetzen, gibt es einige Vorarbeiten sowohl auf dem Exchange Server als auch der Netzwerkinfrastruktur zu erledigen. Dass Sie eine Mindestversion von Exchange benötigen und weitere Abhängigkeiten mit öffentlichen Ordnern beachten müssen, hat Microsoft ausführlich beschrieben. Allerdings ist Exchange nicht das einzige System, welches nicht nur theoretisch angreifbar ist. Es könnte jede Applikation betreffen, die auf dem IIS aufsetzt, NTLM zur Anmeldung akzeptiert und ein Angreifer von einem legitimen Benutzer ein NTLM-Hash abgegriffen hat.

Sie müssen also die komplette Kette aus Client, ausgehenden Proxy, eingehenden Proxy, Loadbalancer etc. betrachten, denn wenn Sie auf dem letzten Server die Funktion "Extended Protection" aktivieren, dann kann dies die Funktion stören. Die TLS-Verbindung muss durchgängig vom Client zum Zielserver existieren und darf nicht aufgebrochen werden. Weder auf der Seite des Clients durch einen ausgehenden Proxy Server noch eingehend beim Ziel durch einen Loadbalancer. Nur dann funktioniert eine HTTPS-Verbindung über "Extended Protection".



Ihre Exchange Umgebung hat in der Regel eine der folgenden Konstellationen:

Ausgehender Proxy

Zuerst betrachten wir uns eine Verbindung zum Exchange Server, bei der ein HTTP-Proxy zum Einsatz kommt. Dies trifft im internen LAN meist nicht zu, aber wenn Sie Exchange Online nutzen oder z.B. einen fremden Client in einem Internet-Cafe oder einen "Cloud-Proxy" nutzen, dann kann das durchaus der Fall sein.

Szenario	Extended Protection

Öffentliche IP-Adresse	In dem Fall sollte es keine Probleme geben. Allerdings gibt es nur ganz wenige Clients, die eine öffentliche IPv4-Adresse haben. Bei IPv6 ist das aber der Regelfall	OK
Private Adresse mit NAT	Der Exchange Server ist per TCP direkt oder per NAT erreichbar. Der Client hat eine durchgängige TCP-Verbindung zum Server	OK
Ausgehender Transparenter Proxy	Der Client muss über einen HTTP-Proxy die Verbindung zum Exchange Server aufbauen. Der Proxy bricht die Verbindung aber nicht auf, sondern erlaubt einen PROXY CONNECT und schaltet den TCP-Stream transparent durch. Das ist auch ein Grund, warum Microsoft für einige Dienste ein "Optimization Required" fordert.	OK
Ausgehender Inspection Proxy	Der Client muss über einen HTTP-Proxy die Verbindung zum Exchange Server aufbauen. Der Proxy terminiert die SSL-Verbindung und baut sie selbst auf, um in die Daten reinzuschauen	Fail

Eingehender Proxy/Loadbalancer

Auf der Seite des Servers können unterschiedliche Zugänge denkbar sein.

Szenario		Extended Protection
Öffentliche IP	Firmen verstecken ihre Server gerne hinter privaten Adressen mit eingehendem NAT aber bei Internet Service Providern haben die Server in der Regel öffentliche IP-Adressen	OK
Eingehender L4-Proxy	Vor dem Exchange Server steht ein Loadbalancer oder eine Firewall, die TCP-Verbindungen auf mehrere Backend Server verteilt oder die Verbindung per NAT (Layer-4) umsetzt. Es ist eine transparente TCP-Verbindung	OK
Eingehender L7-Proxy Bridge 1 Zert	Eingehende Verbindungen werden von Web Application Firewall/Reverse Proxy/Loadbalancer mit dem gleichen Zertifikate terminiert, die auch der Exchange Server nutzt und dann zum Exchange Server wieder verschlüsselt.	OK
Eingehender L7-Proxy Bridge 2 Zert	Eingehende Verbindungen werden von Web Application Firewall/Reverse Proxy/Loadbalancer mit einem anderen Zertifikate terminiert, die auch der Exchange Server nutzt und dann zum Exchange Server wieder verschlüsselt. Das ist gar nicht so selten, dass intern auf dem Exchange Server z.B. Zertifikate einer internen PKI genutzt werden, weil sie billiger sein oder z.B. keine PKI einen Namen für eine ungültige DNS-Domain wie "ex01.firma.local" ausstellt.	Fail
Eingehender L7-Proxy Offload	Sie meinen es gut mit dem Exchange Server und ersparen ihm den SSL-Overhead, indem der Reverse Proxy die Verbindung unverschlüsselt weiterreicht. Hinweis: Diese Konfiguration verhindert auch die Funktion des MRSProxy und damit eine Exchange Hybrid Migration. Für Outlook AnyWhere muss SSL Offloading abgeschaltet werden.	Fail

Abgesehen von noch einigen anderen Abhängigkeiten wie TLS-Konfiguration (TLS 1.2) und NTLMv1-Verzicht (Siehe Checkliste auf Exchange Extended Protection) wird die Aktivierung von Extended Protection nur funktionieren, auf dem Weg von Client zum Exchange sowohl beim ausgehenden als auch bei eingehenden Proxy eine unterstützte Konfiguration vorliegt. Letztlich ist das ja das Prinzip von Extended Protection, dass kein Proxy "reinschauen" und die Daten abgreifen oder verändern kann.

Ich habe noch nicht die Zeit gehabt zu prüfen, ob es es wirklich das "gleiche" Zertifikat sein muss oder ob nur der gleiche Privatekey genutzt werden kann.
In der RFC 5929 steht bei "tls-server-end-point' Channel Binding Type" https://www.rfc-editor.org/rfc/rfc5929.html#section-4, dass das komplette Zertifikat als Hashwerte genutzt wird.

Extended Protection und WCF

Es gibt Dienste, die über den IIS angesprochen werden aber ihrerseits dann nach hinten z.B. per WCF weiter kommunizieren. Der IIS ist hier dann auch nur ein "Reverse Proxy", der vielleicht NTLM durchleitet. Gesehen habe ich dies z.B. bei Zertifizierungsstellen:

- Extended Protection for Authentication Overview
  https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/extended-protection-for-authentication-overview

- Extended Protection Policy
  https://learn.microsoft.com/en-us/dotnet/framework/wcf/samples/extended-protection-policy
- ReadMe for Extended Protection Authentication Sample
  https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/readme-for-extended-protection-authentication-sample?source=recommendations
- WCF Error The ExtendedProtectionPolicy.PolicyEnforcement values do not match
  https://mydevtalks.blogspot.com/2016/07/wcf-error-extendedprotectionpolicypolic.html
- Funktionstest durchführen für den Certificate Enrollment Policy Web Service (CEP)
  https://www.gradenegger.eu/de/funktionstest-durchfuehren-fuer-den-certificate-enrollment-policy-web-service-cep/

Extended Protection mit Exchange und andere

Die Konfiguration von Extended Protection ist im Grund unabhängig von den verschiedenen Diensten, die auf dem IIS aufsetzen. Allerdings ist es immer sinnvoll auch den Hersteller zu fragen, ob Probleme bekannt sind und die Nutzung von EP möglich ist. Dies gilt insbesondere bei der Einstellung "Require", weil dann alle Clients auch EP unterstützen und Nutzen müssen.

Auch wenn "Extended Protection" schon im Jahr 2010 mit einem Update sogar für Windows 2003 bereitgestellt wurde, und auf jedem IIS7.5 und höher damit vorhanden ist, hat Microsoft erst im August 2022 für Exchange Server nicht nur die Freigabe sondern auch die Empfehlung für die Aktivierung gegeben. Im Februar 2024 wurde das Thema dann wieder hochgespült, weil eine Outlook Lücke oder andere MITM-Attacken damit auf Exchange zielen.

Wenn Sie EP aktiviert haben und die Konfiguration nicht passt, dann bekommt die Anwender mit z.B. Outlook immer wieder eine Kennwortbox, die selbst bei der Eingabe korrekter Anmeldedaten nicht funktioniert.

- CVE-2024-21410 Betrachtung
- Exchange Extended Protection
- Kennwortbox
- Extended Protection mit internen Zertifikaten
  So kann ich Extended Protection mit Reverse Proxy und internen Zertifikaten nutzen
- CVE-2024-21410 Microsoft Exchange Server Elevation of Privilege Vulnerability
  https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21410
- CVE-2023-23397 Microsoft Outlook Elevation of Privilege Vulnerability (CVSS score 9,8/9,1)
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
- Guidance for investigating attacks using CVE-2023-23397
  https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/
- Microsoft Mitigates Outlook Elevation of Privilege Vulnerability
  https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/
- Extended Protection for Authentication (December 08, 2009)
  https://msrc.microsoft.com/blog/2009/12/extended-protection-for-authentication/
- Released: 2024 H1 Cumulative Update for Exchange Server
  https://techcommunity.microsoft.com/t5/exchange-team-blog/released-2024-h1-cumulative-update-for-exchange-server/ba-p/4047506
- Configure Windows Extended Protection in Exchange Server
  https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-extended-protection

Allerdings ist das "Problem" einer Man in the Middle-Attacke ja nicht auf Exchange beschränkt, sondern genereller Natur für alle auf dem IIS aufsetzenden Dienste. Dazu gehören z.B. SharePoint OnPremises, WSUS, Skype for Business, ADFS und auch viele 3rd-Party-Lösungen, die als ASP/ASPX/PHP-Seite auf dem IIS laufen und die "Windows Authentifizierung" nutzen. Es betrifft aber auch andere Dienste wie LDAP, die ebenfalls TLS nutzen.

- LDAP Security: LdapEnforceChannelBinding
- 2020, 2023, and 2024 LDAP channel binding and LDAP signing requirements for Windows (KB4520412)
  https://support.microsoft.com/en-gb/topic/2020-2023-and-2024-ldap-channel-binding-and-ldap-signing-requirements-for-windows-kb4520412-ef185fb8-00f7-167d-744c-f299a66fc00a
- Secure domain controllers with LDAP channel binding and LDAP signing
  https://4sysops.com/archives/secure-domain-controllers-with-ldap-channel-binding-and-ldap-signing/
- NTLM - New Technology LAN Manager & the attack possibilities
  https://www.prosec-networks.com/en/blog/ntlm-new-technology-lan-manager/

Einen Marktüberblick habe ich hier nicht und so kann ich ihnen nur raten, EP einfach einzuschalten und zu kontrollieren, welche Client über welche Authentifizierung die Dienste nutzen. Achten Sie darauf, dass wirklich auch NTLM zum Einsatz kommt und kein anderes Anmeldeverfahren.

Extended Protection und Clients

Damit Extended Protection überhaupt zum Einsatz kommt, muss die Windows Authentifizierung genutzt werden. Anmeldungen eines Clients per BasicAuth, Digest, FormBased oder Bearer sind nicht betroffen. Daher ist es in den meisten Fällen der Edge-Browser oder Anwendungen wie Outlook, die per HTTPS und NTLM auf OnPremises Dienste zugreifen.

Ich weiß, dass die aktuellen Microsoft Office Produkte und der Microsoft Edge Server auch Extended Protection unterstützen. Leider habe ich noch kein Übersicht zu anderen Produkten oder genauen Versionen gefunden. Aber aus Release Notes habe ich folgendes zusammengesucht.

Client	Status	Beschreibung und Links
Edge (Chromium)	Ja	Support tls-server-end-point channel bindings for HTTP authentication. (Closed) https://codereview.chromium.org/1408433006/patch/100001/110039
Chrome (Chromium)	Ja	Support tls-server-end-point channel bindings for HTTP authentication. (Closed) https://codereview.chromium.org/1408433006/patch/100001/110039
Thunderbird	Ab Version 41 (2016)	thunderbird 38.0.1: cannot send email through exchange server (NTLM) https://bugzilla.mozilla.org/show_bug.cgi?id=1174159
Firefox	Ab Version 11 (2011)	Enable Extended Protection (channel and service binding) for NTLM authentication https://bugzilla.mozilla.org/show_bug.cgi?id=573043

Letztlich kommt es auf einen Versuch an.

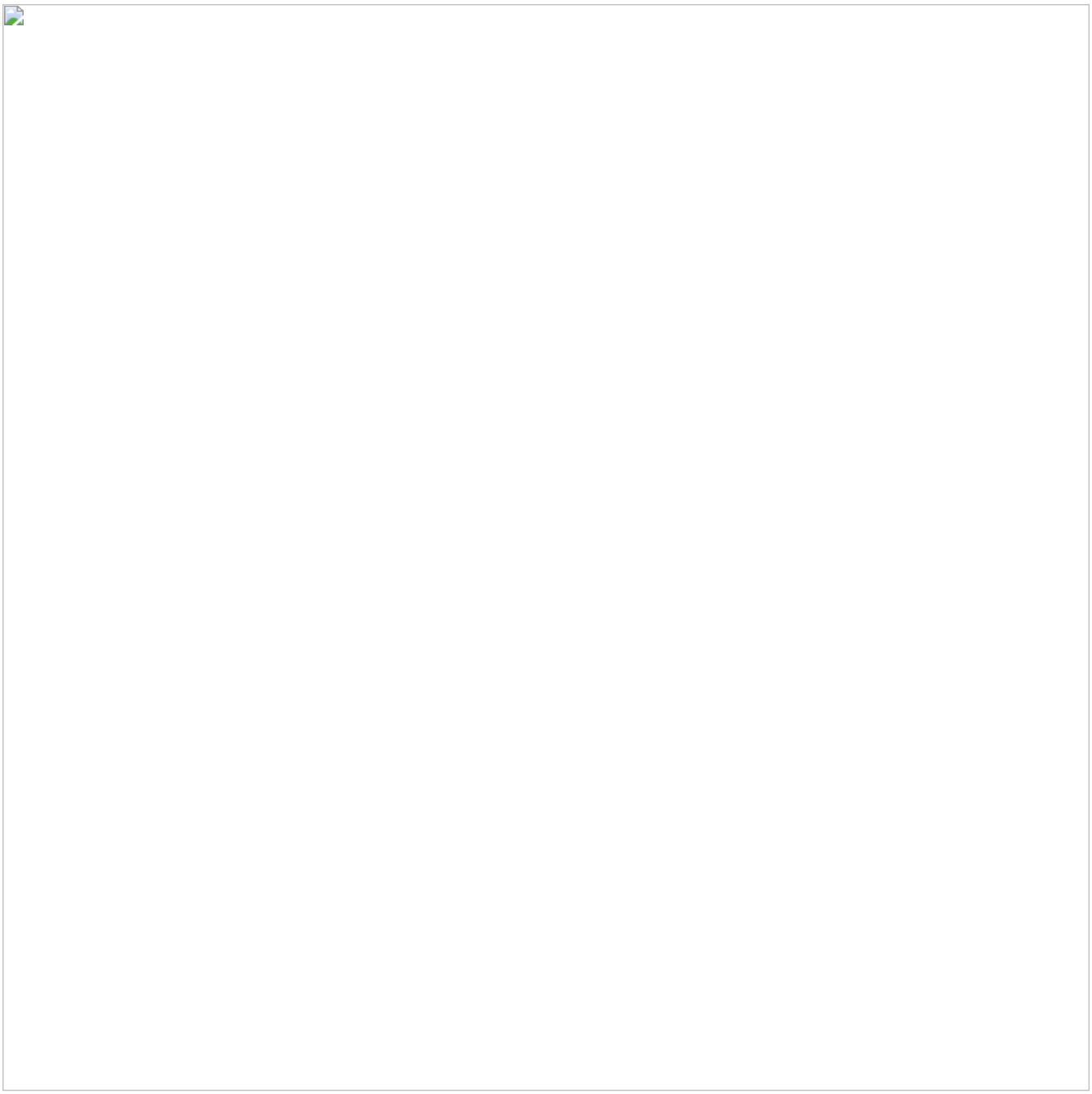
Note: The Extended Protection authentication setting on Windows is used to configure Kerberos mutual authentication. In this type of authentication, to prevent a man-in-the-middle attack, the server authenticates to the client and the client authenticates the server. Windows 7 on Firefox doesn't support Extended Protection. If users use this client configuration disable Extended Protection in ADFS.
Quelle: Enabling Integrated Windows Authentication in Firefox
https://help.hcltechsw.com/domino/11.0.1/admin/secu_enabling_iwa_in_firefox.html

- Extended Protection for Authentication (December 08, 2009)
  https://msrc.microsoft.com/blog/2009/12/extended-protection-for-authentication/
- SEC_CHANNEL_BINDINGS structure (sspi.h)
  https://learn.microsoft.com/en-us/windows/win32/api/sspi/ns-sspi-sec_channel_bindings
- 3.2.1.4.1.1 Using a Security Context
  https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rpce/6b733b95-3fd9-4ad5-ba4f-28e548db1c24

Extended Protection im IIS aktivieren

Für Exchange sollten Sie nicht direkt im IIS die Konfiguration ändern, sondern laut Beschreibung von Microsoft zuerst mit dem Exchange HealthChecker ihre Konfiguration prüfen und dann entweder durch die Installation von Exchange 2019 CU14 die Konfiguration anpassen lassen. Alternativ können Sie dies auch durch entsprechende PowerShell-Befehle durchführen.

Für alle anderen Fälle finden Sie die Einstellung im Bereich "Authentication" auf der Webseite und jedem virtuellen Verzeichniss. Von den verschiedenen Anmeldeverfahren ist die "Windows Authentication" und dann "Advanced Settings" zu wählen.



Hier können Sie drei Optionen auswählen:

- Off
  Der Server bietet EP gar nicht an.
- Accept
  Der Server bietet EP an und wenn es der Client nutzen möchte, ist es möglich. Ich bin nicht sicher, ob hier ein Proxy das Angebot unterdrücken könnte. Aber Accept ist aus meiner Sicht auch nicht sicher, da es ja nicht erzwungen wird.
- Require
  Der Server erzwingt, die Verwendung von EP. Der Client muss es unterstützen und Proxy-Systeme dürfen nichts aufbrechen.

Microsoft stellt bei Exchange die EP-Funktion nicht bei allen Verzeichnissen ein, sondern nur solche, bei denen einen Zugriff per Windows Authentication möglich ist. Bei den anderen Verfahren ist es nicht möglich.

- Erweiterter Schutz für Windows <extendedProtection>
  https://learn.microsoft.com/de-de/iis/configuration/system.webserver/security/authentication/windowsauthentication/extendedprotection/
- KB5021989: Extended Protection for Authentication
  https://support.microsoft.com/en-au/topic/kb5021989-extended-protection-for-authentication-1b6ea84d-377b-4677-a0b8-af74efbb243f
  Achtung: EP kann man per Regedit und den Schlüssel "SuppressExtendedProtection" auch abschalten:

Ich habe bislang weder in Fiddler noch im Chromium Debugger einen Weg gefunden zu sehen, ob EP angeboten oder genutzt wird. Da es aber eine TLS-Erweiterung ist, wäre wohl Wireshark der bessere Ansatzpunkt.

Extended Protection "testen"

Sie wissen nun, wie Extended Protection im Grunde funktioniert und wie es aktiviert wird. Dennoch wird der vorsichtige Administrator dies erst einmal testen wollen. Dies ist mit dem IIS relativ einfach möglich:

1. neues virtuelles Verzeichnis
   Legen Sie z.B. "/test" an.
2. Testdatei
   Legen Sie dort eine Datei "default.htm" an, in der sie einfach einen kurzen Test schreiben.
3. Authentication = Negotiate mit NTLM + EP
4. 4. Veröffentlichung über HLB/Proxy
   Zuletzt machen Sie das "/Test"-Verzeichnis über ihren Loadbalancer oder Reverse Proxy erreichbar
5. 5. Zugriff per Browser
   Nun surfen Sie die Seite per Browser an. Sie sollten im Browser Debugger gut sehen, dass die Anmeldung per NTLM erfolgt, z.B. an zwei 401-meldnugen vor der 200 Meldung und den Einträgen im Header

Sie können mit dem Verzeichnis weitere Konstellationen durchspielen.

Weitere Links

- CVE-2024-21410
- CVE-2023-23397 - Microsoft Outlook Elevation of Privilege Vulnerability
- Exchange Extended Protection
- Extended Protection mit internen Zertifikaten
  So kann ich Extended Protection mit Reverse Proxy und internen Zertifikaten nutzen
- MRS und Extended Protection
  Wenn EXO mit NTLM auf fehlerhaftes Extended Protection trifft
- Checkliste Active Directory Absicherung
  Keine Liste ist komplett aber fangen Sie heute an und hören sie nie auf
- TLS Security
- SSL-Inspection
- TLS Handshake
- TLS 1.2 Enforcement
- Verschlüsseln und Signieren
- Private Key
- Gruppenrichtlinien
- WPAD - Proxy im Browser einstellen
- Fiddler
- Bearer Decoding
- HTTP Proxy Authentication
- X-Forwarded-For
- Azure AD Application Proxy
- HTTP Authentication
- Description of the update that implements Extended Protection for Authentication in Internet Information Services (IIS)
  https://support.microsoft.com/en-us/topic/description-of-the-update-that-implements-extended-protection-for-authentication-in-internet-information-services-iis-0efdf83b-2ae5-040c-5308-6cacf2e24b30
- Extended Protection for Authentication Overview
  https://learn.microsoft.com/en-us/dotnet/framework/wcf/feature-details/extended-protection-for-authentication-overview
- Extended Protection for Authentication (December 08, 2009)
  https://msrc.microsoft.com/blog/2009/12/extended-protection-for-authentication/
- Released: 2024 H1 Cumulative Update for Exchange Server
  https://techcommunity.microsoft.com/t5/exchange-team-blog/released-2024-h1-cumulative-update-for-exchange-server/ba-p/4047506
- EP setup documentation
  https://aka.ms/ExchangeEPDoc
- Coming Soon: Enabling Extended Protection on Exchange Server by Default
  https://techcommunity.microsoft.com/t5/exchange-team-blog/coming-soon-enabling-extended-protection-on-exchange-server-by/ba-p/3911849
- 2020, 2023, and 2024 LDAP channel binding and LDAP signing requirements for Windows (KB4520412)
  https://support.microsoft.com/en-gb/topic/2020-2023-and-2024-ldap-channel-binding-and-ldap-signing-requirements-for-windows-kb4520412-ef185fb8-00f7-167d-744c-f299a66fc00a

- Channel Binding: Should you be using it?
  https://csb.stevekerrison.com/post/2022-01-channel-binding/
- KB5021989: Extended Protection for Authentication
  https://support.microsoft.com/en-au/topic/kb5021989-extended-protection-for-authentication-1b6ea84d-377b-4677-a0b8-af74efbb243f
  Achtung: EP kann man per RegEdit und den Schlüssel "SuppressExtendedProtection" auch abschalten:
- RFC 5929: Channel Bindings for TLS
  https://www.rfc-editor.org/rfc/rfc5929.html
- RFC 5056: On the Use of Channel Bindings to Secure Channels
  https://www.rfc-editor.org/rfc/rfc5056
- Wikipedia: Token Binding
  https://en.wikipedia.org/wiki/Token_Binding
- Cain & Abel
  https://de.wikipedia.org/wiki/Cain_%26_Abel

Tags: IIS Extended Protection NTLM