Die sichere, intuitive
und reibungslose Zusammenarbeit

BenQ InstaShow®

Security Guide

1. Zusammenfassung

Angesichts der rasanten Entwicklung von Netzwerkprodukten und Trends für ein papierloses, drahtloses Büro entscheiden sich immer mehr Unternehmen für die Einführung von WPS. Die einfache Bildschirmprojektionstechnologie von WPS ermöglicht es den Konferenzteilnehmern, den Aufwand für das Anschließen von Kabeln an einen Monitor zu vermeiden. Stattdessen können sie den Bildschirm drahtlos von ihrem persönlichen Gerät aus nutzen. Die Technologie ermöglicht eine neue Art der Präsentation und Zusammenarbeit in Unternehmensumgebungen.

Während Sie mit WPS die Bequemlichkeit drahtlos verbundener Produkte genießen können, müssen Sie jedoch auch wissen, ob die Daten während der drahtlosen Übertragungen ordnungsgemäß geschützt sind. Wir teilen die Bedrohungen für die Informationssicherheit, die bei der Verwendung von WPS häufig auftreten, in zwei Kategorien ein: 1. Datenverletzungen während der Übertragung und 2. Netzwerkinfiltration über die WPS-Wi-Fi-Verbindung. Bei der ersten Bedrohung werden in der Regel die Schwachstellen zwischen dem drahtlosen WPS-Sender und -Empfänger ausgenutzt; die zweite Bedrohung kann die Schwachstellen des Wi-Fi-Netzwerks ausnutzen, um auf drei Arten einzudringen: 1. Verwendung des WPS-Empfänger-Hosts, um in das Unternehmensintranet einzudringen, 2. Verwendung der auf dem Computer installierten WPS-Treiber-App, um Scans durchzuführen oder Backdoor-Schadcode zu implantieren, 3. Verwendung der SSID-Funktion, die bei der Verwendung der drahtlosen Projektion mit der WPS verbunden sein muss, um den mit RX verbundenen Computer zu infiltrieren.

BenQ InstaShow WPS verwendet einen 3-Schicht-Schutzmechanismus., einschließlich 1. Der unabhängige Router muss nicht mit dem Intranet des Unternehmens verbunden werden, und mit Plug-and-Play ist keine Software-Installation erforderlich, 2. die Daten werden vor der Übertragung verschlüsselt. 3. Er hat die Schwachstellenprüfung im Zertifizierungslabor bestanden und vermeidet so die Risiken von Sicherheitslücken im Netzwerk und die Einschleppung von Viren, die leicht durch angeschlossene Produkte verursacht werden können. Als Nächstes werden wir die im vorigen Abschnitt erwähnten potenziellen Schwachstellen von WPS erläutern, die wir in zwei Aspekte unterteilen: Datenverletzung und Netzwerkinfiltration. Und wir werden erörtern, wie der von BenQ InstaShow verwendete 3-Schichten-Schutzmechanismus Schwachstellen vermeidet, Bedrohungen der Informationssicherheit effektiv reduziert und die Datensicherheit erhöht.

1. Häufige Schwachstellen in WPS

1.1 Bedrohung durch Datenverletzungen

Bei der WPS-Übertragung zwischen Sender und Empfänger kann es vorkommen, dass Daten versehentlich durch Abhören abgefangen werden. Dies ist eine der potenziellen Bedrohungen für die Datensicherheit.

Die Unterschiede zwischen kabelgebundener und kabelloser Nutzung

WPS überträgt die Informationen des Senders über eine drahtlose Technologie an den Empfänger. Der Sicherheitsunterschied zwischen der Verwendung von WPS und kabelgebundenem HDMI besteht darin, dass das normale kabelgebundene HDMI-Signal direkt an den Monitoreingang übertragen wird, ohne dass ein Dritter dazwischengeschaltet wird. Obwohl kabelgebundene Verbindungen unbequem sein können, fühlen sich die Menschen damit sicherer als bei der Verwendung von drahtlosen Verbindungen, bei denen das vom Laptop zum Empfänger gesendete Signal abgefangen werden kann.

Die herkömmliche Verwendung von WiFi in WPS weist die folgenden Schwachstellen auf, und die üblichen Methoden zur Offenlegung sind wie folgt:

	HDMI Kabel	**Drahtloses Präsentationssystem**
Umfang des Abhörens	Selber Meetingraum	Verschiedene Besprechungsräume, sofern ein Wireless AP-Signal erkannt werden kann
Den Dieben zur Verfügung stehende Methoden	Vertrauliches Briefing durch Handykamera	1. Unauthentifizierter Sender: Getarnt als Gerät eines Mitarbeiters (Laptop) und Abfangen aller Netzwerkpakete, die an das Gerät des Mitarbeiters gesendet werden 2. Ungesichertes drahtloses Netzwerk: Zeichnet wahllos alle drahtlosen Pakete in der Luft auf, bevor er sie knackt

Tabelle 1: Vergleichstabelle der Datenverletzungen mit HDMI-Kabel und WPS

Einfach ausgedrückt, ist die Ursache für solche Datenverletzungen ein nicht authentifizierter Sender. Ein gefälschter Sender sendet eine Schlüsselanforderung an den Empfänger des WPS-Systems. Da der Empfänger den gefälschten Sender nicht identifizieren kann, wird der Schlüssel für die Anfrage gesendet. Auf diese Weise kann der gefälschte Sender erfolgreich die Ver- und Entschlüsselungs-schlüssel erhalten und alle vom Sender gesendeten verschlüsselten Dateien knacken.

Eine weitere Ursache für Datenverletzungen sind unsichere drahtlose Netzwerke. Wahlloses Aufzeichnen aller Netzwerkpakete durch einen drahtlosen Sniffer. Abbildung 1 unten beschreibt die Überwachung von Paketen zwischen Bon und Alice über das Netzwerk. Hacker können wertvolle Inhalte aufzeichnen und herausfiltern.

Eine Analogie:

Der Reisepass von Herrn Li wird von einer illegalen Gruppe in Dubai gestohlen. Herr Zhang, ein Mitglied der illegalen Gruppe, nimmt fälschlicherweise die Identität von Herrn Li an und geht zum Büro in Dubai, um einen vorläufigen Reisepass zu beantragen. Herr Zhang ist wie ein falscher Sender (Herr Li in Verkleidung), und das Büro in Dubai ist der Empfänger. Der falsche Herr Li bittet das Büro in Dubai um eine Neuausstellung seines Passes, was einer Bitte um Verschlüsselungs- und Entschlüsselungsschlüssel gleichkommt. Nachdem Herr Zhang einen neuen Pass (d. h. Verschlüsselungs- und Entschlüsselungsschlüssel) erhalten hat, ist dies so, als würde er Herrn Lis Identität knacken. Es ist nicht nur möglich, Herrn Li auf Schritt und Tritt zu verfolgen, sondern auch unter seiner Identität illegale Aktivitäten zu unternehmen.

Abbildung 1: Datenschutzverletzungen durch ein unsicheres Netz

1.1.2 Unterschiede zwischen dem USB- und dem HDMI-Button

Bei herkömmlichen WPS wird ein spezieller Sender oder eine App verwendet. Derzeit ist der beliebteste Sender die Buttonform, die es dem Präsentator ermöglicht, eine Taste zu drücken, um den Bildschirm drahtlos anzuzeigen; ein Beispiel hierfür ist BenQ InstaShow®.

Es gibt zwei Hauptschnittstellen für das Videostreaming über eine Schaltfläche: 1. USB-Anschluss, 2. HDMI-Anschluss:

TX-Button Schnittstelle	**USB Button (Nicht BenQ)**	**HDMI Button (BenQ)**
Umfang des Abhörens/Abfangens	Verschiedene Besprechungsräume, sofern ein Wireless AP-Signal erkannt werden kann	Verschiedene Besprechungsräume, sofern ein Wireless AP-Signal erkannt werden kann
Den Dieben zur Verfügung stehende Methoden	1. Die "Hintertür" wird durch das Hacker-Tool im Voraus in die Taste implantiert und dann wieder eingesetzt, so dass uninformierte Benutzer nun die "Hintertür"-Taste verwenden. 2. Einschleusen der bösartigen Codes in den Computer des Mitarbeiters über den USB-Anschluss (wird im nächsten Kapitel erläutert).	Der bösartige Backdoor-Code kann den HDMI-Button nicht kompromittieren; dies ist nur über das Abhören der Funkverbindung möglich.

Tabelle 2: Vergleich zwischen USB-Taste und HDMI-Taste

1.2 Netzwerk-Infiltration

Eine weitere Sicherheitsbedrohung für das WPS-System ist die Infiltrierung des Unternehmensnetzwerks. Zu den Infiltrationspfaden gehören: 1. Verwendung des WPS-Empfänger-Hosts, um in das Unternehmensintranet einzudringen, 2. Verwendung der auf dem Computer installierten WPS-Treiber-App, um Scans durchzuführen oder Backdoor-Schadcode zu implantieren, 3. Verwendung der SSID-Funktion, die mit der WPS verbunden sein muss, wenn eine drahtlose Projektion verwendet wird, um den mit RX verbundenen Computer zu infiltrieren.

WPS wird als Netzwerkkommunikationsgerät eingestuft. Aufgrund der Eigenschaften von Netzwerkgeräten können Benutzer, die sich mit WPS oder WPS-Geräten, die sich mit dem Intranet verbinden, verbinden, dem Unternehmen Schaden zufügen.

Für Bedrohungen, die über WPS in das Unternehmensintranet eindringen, haben wir die folgenden Vorkehrungen je nach Eindringtiefe und Angriffsmethode getroffen:

Tabelle 3: Arten der Netzinfiltration

Methode	Angriffs-methode	Mögliche Risiken	Umfang des Abhörens	Ergebnisse
1. WPS EMPFÄNGER Host: Die Unternehmen sind daran gewöhnt, das WAN der Empfangs-geräte mit dem Intranet des Unternehmens zu verbinden, um die Netzkontrolle zu erleichtern.	Verweigerung von Diensten	Das Empfangsgerät selbst birgt das Risiko von Systemschwachstellen und Exploits	Intranet oder Extranet des Unternehmens	Schwachstellen werden von Personen ausgenutzt, die beabsichtigen, in das Unternehmen einzudringen oder die Ausstattung des Unternehmens anzugreifen
2. Personal-PC/Gäste-PC: Drahtlose Präsentations-App verwenden und installieren	Scannen	Die App verwendet ein bestimmtes Netzwerk	Unternehmens-intranet (Gäste bringen es in ihr eigenes Unternehmen zurück)	Personen, die die Absicht haben, das drahtlose Projektions-App-Netzwerk zu nutzen, um in das Unternehmensintranet einzudringen und Daten zu stehlen oder das Unternehmensintranet anzugreifen
	Backdoor-Schadcode	Auf einer gefälschten App installieren	Unternehmensintranet	Personen, die die Absicht haben, das drahtlose Projektions-App-Netzwerk zu nutzen, um einen bösartigen Code durch eine Hintertür einzuschleusen und Daten zu stehlen oder das Unternehmens-intranet anzugreifen
Personal-PC/Gast-PC: Um die drahtlose Präsentation zu nutzen, verbinden Sie das Gerät mit der SSID des Empfängers oder des Firmenintranets	Scannen + Backdoor-Schadcode	Infizierte Geräte im Intranet des Unternehmens versuchen, über den Empfänger auf den Computer des Gastes zuzugreifen	Unternehmensintranet (Gäste bringen es in ihr eigenes Unternehmen zurück)	Böswillige Personen nutzen den infizierten Computer im Unternehmen, um eine Verbindung zum infizierten Empfänger herzustellen, und verbreiten sich dann auf die mit dem Empfänger verbundenen Geräte, um Backdoor-Programme zu implantieren und Daten zu stehlen.

Hacker nutzen WPS, um in das Unternehmensnetz einzudringen und Folgeangriffe zu starten. Das "Scannen" ist in der Regel ein Vorspiel zur Infiltration. Die beim Scannen gefundenen Schwachstellen werden zu Pfaden für die Infiltration. Nach der Infiltration folgen Backdoor-Schadcode-Intrusionen, Denial-of-Service-Angriffe und gemischte Angriffe.

2. 2. BenQs 3-Ebenen-Ansatz

Wie schützt BenQ vor möglichen Schwachstellen in WPS?
Zunächst stellen wir das dreiteilige Designkonzept von BenQ vor, von der äußeren bis zur inneren Sicherheitsebene.

Abbildung 2: Der 3-Ebenen-Ansatz von BenQ Instashow® für Sicherheit

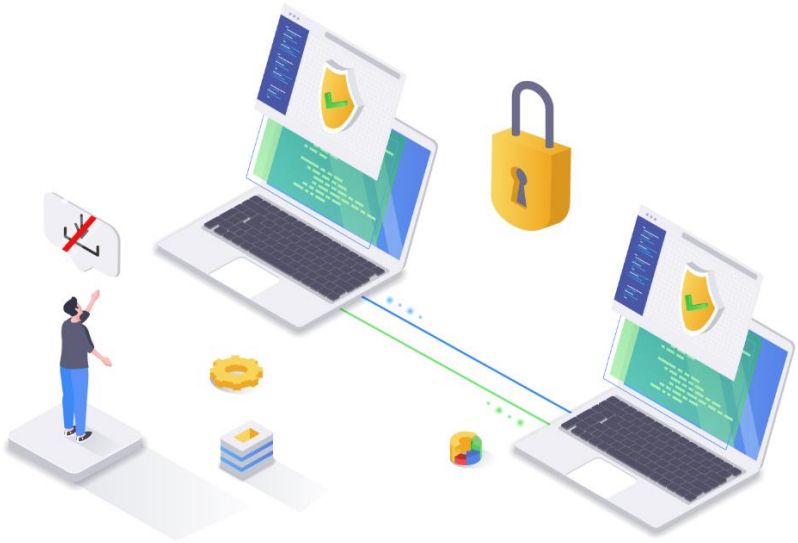
Ebene	Entsprechende Bedrohung	Entsprechende Schwachstellen in der Informationssicherheit und Anti-Blocking-Ziele	Lösungen
Ebene 1: Drahtlose Datenverschlüsselung	Datenpanne	Übertragungen zwischen Sender und Empfänger werden überwacht	· WPA3 Datenverschlüsselung · CC EAL6+ Eingebauter Hardware-Sicherheitschip · FIPS 140-3 CAVP-zertifizierte Verschlüsselung
Ebene 2: Isoliertes System	Infiltration des Netzes	· Das Firmen-Intranet wird über die Verbindungsfunktionen zwischen WPS und dem Firmen-Intranet infiltriert; oder die WPS wird vom Firmen-Intranet aus infiltriert. · Über die auf dem Computer installierte WPS-Treiber-APP wird Code zum Scannen nach Schwachstellen oder bösartiger Backdoor-Code eingeschleust.	· Router-Chipsatz mit Firewall-Funktion zum Blockieren externer Angriffe · Mit einem unabhängigen Router-AP ist keine Verbindung zum Unternehmensintranet erforderlich · Der Sende-Button ist Plug-and-Play, sodass keine Softwareinstallation erforderlich ist.
Ebene 3: CVSS v3 Vulnerability Bewertung	Infiltration des Netzes	Wenn Hacker den Empfänger nach Schwachstellen durchsuchen, können sie die entdeckten Schwachstellen nutzen, um sich einzuschleichen.	Schwachstellen-Scans und Korrekturen durch zertifizierte Labors

Tabelle 4: Der 3-Ebenen-Ansatz von BenQ Instashow zur Sicherheit

Ebene 1 - Drahtlose Datenverschlüsselung

Als Reaktion auf die Bedrohung durch Datenschutzverletzungen, die durch die Überwachung hervorgerufen werden, verwendet BenQ InstaShow die neueste drahtlose Wi-Fi 6-Technologie, um die drahtlosen Übertragungen von der branchenüblichen WPA2-Verschlüsselung auf WPA3 zu aktualisieren. Solange das Mobiltelefon oder der Laptop WPA3 unterstützt, kann die drahtlose Verschlüsselung auf WPA3 aufgerüstet werden, egal ob BenQ InstaShare oder Airplay oder Chromecast-Projektion verwendet wird.

1. Exchanging the Certificates

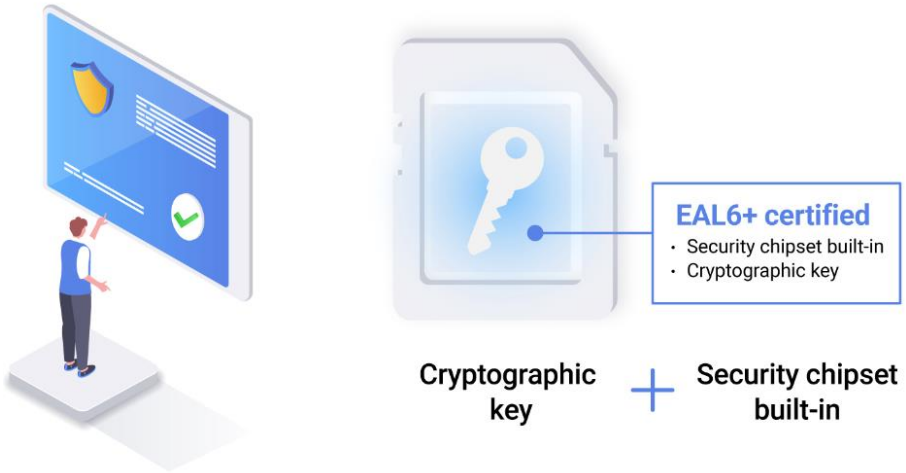


Zwei-Wege-Authentifizierung zwischen Sender und Empfänger mit gegenseitigen Handshakes (über den Austausch von Zertifikaten)

2. Create Encrypted Tunnel

1. Bevor der Button an den Empfänger übermittelt wird, muss er bestätigen, dass der Empfänger der richtige Zusteller ist.
2. Bevor der Empfänger den Button annimmt, muss er bestätigen, dass der Button ein rechtmäßiger Empfänger ist.
Sobald die zweiseitige Authentifizierung abgeschlossen ist, erstellt das System einen verschlüsselten Tunnel.

3. Extra Security for Data Encryption



Nach der Authentifizierung werden die Verbindung und die nachfolgenden Datenübertragungen durch den FIPS 140-3-zertifizierten kryptografischen Algorithmus und den EA6+-zertifizierten Chipsatz von InstaShow WDC30 geschützt (wobei der kryptografische Schlüssel auf einem EAL6+-zertifizierten Sicherheitschipsatz gespeichert ist).

Darüber hinaus empfehlen wir für Branchen wie Finanz- und Bankwesen, Behörden, medizinische Versorgung und sogar Produktionslieferketten, in denen drahtlose Präsentationsinhalte hochsensibel sind, keine Software-(App-)Projektionsmethoden wie Airplay oder Chromecast zu verwenden; stattdessen wird die Verwendung der exklusiven Hardware-Senderbutton von BenQ InstaShow zur Projektion des Bildschirms empfohlen. Der Grund dafür ist, dass der BenQ InstaShow Transmitter Button über einen FIPS 140-3 CAVP-zertifizierten Verschlüsselungs- und Entschlüsselungsalgorithmus zwischen dem Sender und dem Empfänger verfügt, der vom National Institute of Standards and Technology (NIST) zertifiziert ist. Dieses Design ähnelt dem Prinzip der Authentifizierung in einer Chip-Kreditkarte oder Smartcard, d.h. es gibt einen hardwarebasierten Sicherheitschipsatz. Der BenQ InstaShow Receiver verfügt über einen eingebauten ISO15408 (Common Criteria) EAL6+ zertifizierten Hardware-Verschlüsselungschip, um die Sicherheit der verschlüsselten Dateien zu gewährleisten, d.h. selbst wenn die Dateien überwacht und angegriffen werden, können sie verschlüsselt bleiben. Darüber hinaus verfügen der FIPS 140-3 CAVP-Algorithmus und der EAL6+-zertifizierte Verschlüsselungschip über die folgenden Merkmale:

1) Überprüfen Sie die Legitimität der Sendung - nicht genehmigte Sendungen können nicht auf dem Bildschirm angezeigt werden.

Sitzungsbasierter Schlüssel - Jede TX-Verbindung verwendet einen neuen kryptografischen Schlüssel zur Verschlüsselung jeder drahtlosen Übertragung, so dass

gewährleistet ist, dass jede TX-Verbindung einen anderen Schlüssel für die Verschlüsselung erhält.

Ebene 2 - Isoliertes System

Für das Scannen und Backdoor von Schadcodes verfügt der BenQ InstaShow Receiver über einen eingebauten routerbasierten Chipsatz. Der größte Vorteil des routerbasierten Chipsatzes ist, dass er eine Firewall-Funktion hat. Durch die Einstellung der Router-Firewall kann der Receiver vom Unternehmensnetzwerk getrennt werden, wodurch verhindert wird, dass unbekannte Quellen von außen in den Receiver eindringen und bösartige Programme in Laptops und andere Geräte, die das drahtlose Präsentationssystem nutzen, einschleusen können.

1) Es kann verhindern, dass Hacker auf Gastcomputer zugreifen, nachdem sie über das Unternehmensintranet und das RX-WAN in den RX gelangt sind.
2) Es kann verhindern, dass Hacker den Computer des Gastes abfragen und erreichen, indem sie sich direkt mit dem RX verbinden

Ein weiterer Aspekt des isolierten Systems bedeutet, dass keine Software oder App erforderlich ist. Softwaretreiber sind immer eine der Hauptquellen für Sicherheitsbedrohungen, vom Softwarefehler selbst bis hin zum Downloadverhalten, das die Öffnung des WIFI-Netzwerks für Gastbenutzer erfordert. Das echte Plug-and-Play Instashow schützt nicht nur die Geräte, an die die Instashow-Button angeschlossen sind, sondern isoliert sich auch vom Unternehmensnetzwerk.

Ebene 3 - Schwachstellenbewertung auf der Grundlage von CVSS v3

WDC30 wird an das Zertifizierungslabor für Informationssicherheit geschickt, um eine Schwachstellenprüfung auf der Grundlage von CVSS v3 in der Entwurfsphase durchzuführen; bekannte Schwachstellen werden in der Entwicklungsphase behoben, um die Robustheit des RX-Systems zu gewährleisten. Die Benutzer profitieren von dem CVSS-Ansatz, da alle Schwachstellen, die nach der Implementierung gepatcht werden müssen, vermieden werden. Die meisten Hersteller von drahtlosen Präsentationssystemen haben es versäumt, Sicherheitsaspekten in der Entwurfsphase Vorrang einzuräumen, was in der Regel zu teuren Nacharbeiten führte, wenn Schwachstellen gefunden und nachträglich gepatcht wurden.

3. Prüfung, Validierung und verantwortungsvolle Offenlegung

Der dreistufige Schutzmechanismus von BenQ InstaShow wurde von einem unabhängigen Labor zertifiziert und entspricht den internationalen Vorschriften zur Informationssicherheit.

Gegenwärtig ist die gesamte InstaShow-Serie mit einem 3-Ebenen-Schutzmechanismus ausgestattet. Die Kunden können je nach Sensibilität ihrer Daten das passende Modell wählen:

Ebene	WDC10 Serie	WDC20 Serie	WDC30 Serie
Ebene 1: Drahtlose Datenverschlüsselung	· WPA2 · HDCP Adoption	· WPA2 · HDCP Adoption	· WPA3 · HDCP Adoption · FIPS 140-3 CAVP zertifiziert Abbildung 3: BenQ InstaShow WDC30 ist zertifiziert nach FIPS140-3 CAVP · EAL6+ Hardware Sicherheitschip Abbildung 4: Eingebauter Hardware-Sicherheitschipsatz
Ebene 2: Isoliertes System	Firewall eingebettet Router-basierter Empfänger AP Abbildung 5: Router-Level-Chip mit Qualcomm- oder MTK-Technologie	Firewall eingebettet Router-basierter Empfänger AP Abbildung 5: Router-Level-Chip mit Qualcomm- oder MTK-Technologie	Firewall eingebettet Router-basierter Empfänger Abbildung 5: Router-Level-Chip mit Qualcomm- oder MTK-Technologie
Ebene 3: CVSS v3 Vulnerability Bewertung	PASS Abbildung 6: Common Vulnerability Score System (CVSS) Zertifikat	PASS Abbildung 6: Common Vulnerability Score System (CVSS) Zertifikat	PASS Abbildung 6: Common Vulnerability Score System (CVSS) Zertifikat

Tabelle 1: Sicherheitszertifikate von BenQ Instashow®

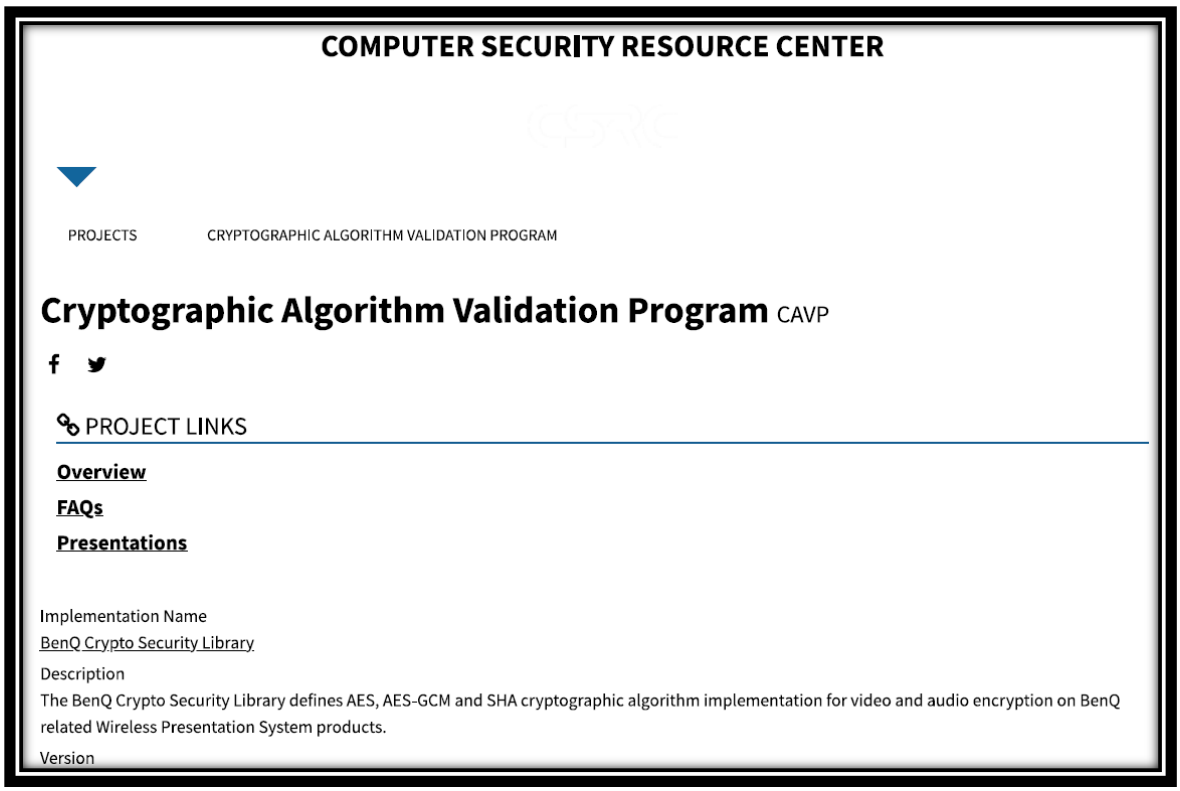


Abbildung 3: BenQ InstaShow WDC30 ist zertifiziert nach FIPS140-3 CAVP [1]

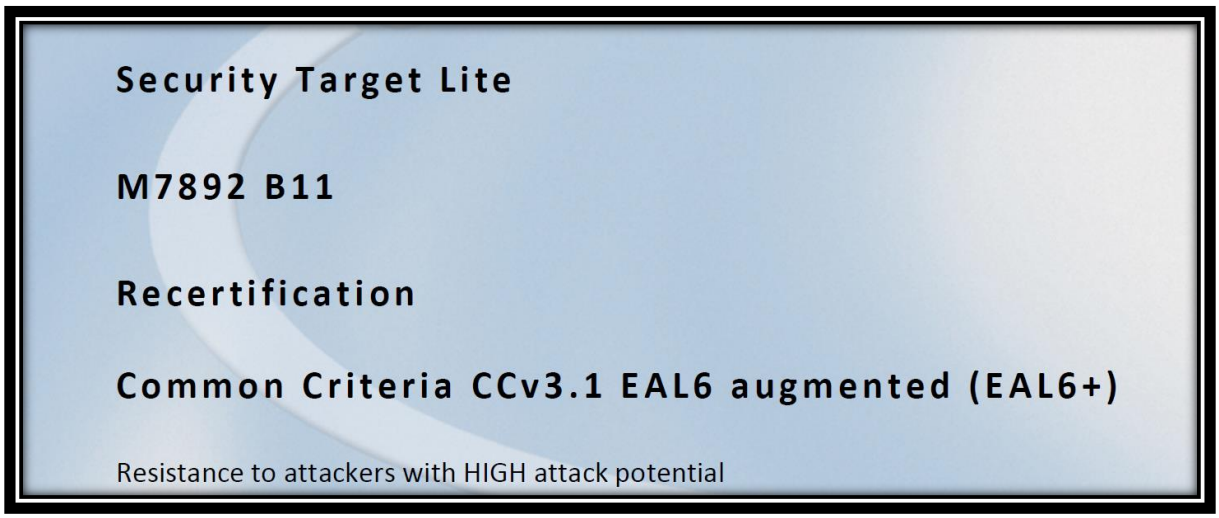


Abbildung 4: Eingebauter Hardware-Sicherheitschipsatz [2]

[1] Quelle: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=14470

[2] Quelle: Bitte kontaktieren Sie BenQ, wenn Sie weitere Informationen benötigen.

Abbildung 5: Router-Level-Chip mit Qualcomm- oder MTK-Technologie [3]

Abbildung 6: Common Vulnerability Score System (CVSS) Zertifikat

[3] Quelle: Bitte kontaktieren Sie BenQ, wenn Sie weitere Informationen benötigen

Anhang

Wir erklären, wie WPS als Schwachstelle in einem drahtlosen Netzwerk genutzt wird, um Denial-of-Service-, Scan- und Backdoor-Schadcode auszuführen.

Verweigerung von Diensten

Nachdem er in das interne Netzwerk des Unternehmens eingedrungen ist, indem er die Schwachstelle des RX-Systems ausgenutzt hat, greift er den internen Mailserver des Unternehmens an, legt ihn lahm und macht ihn unfähig, E-Mails zu senden und zu empfangen; oder er lauert im Extranet des Unternehmens als Mitglied der Bot-Farm des Hackers und wird von Zeit zu Zeit zum Sprungbrett für große Bot-Angriffe auf die Website des Unternehmens.

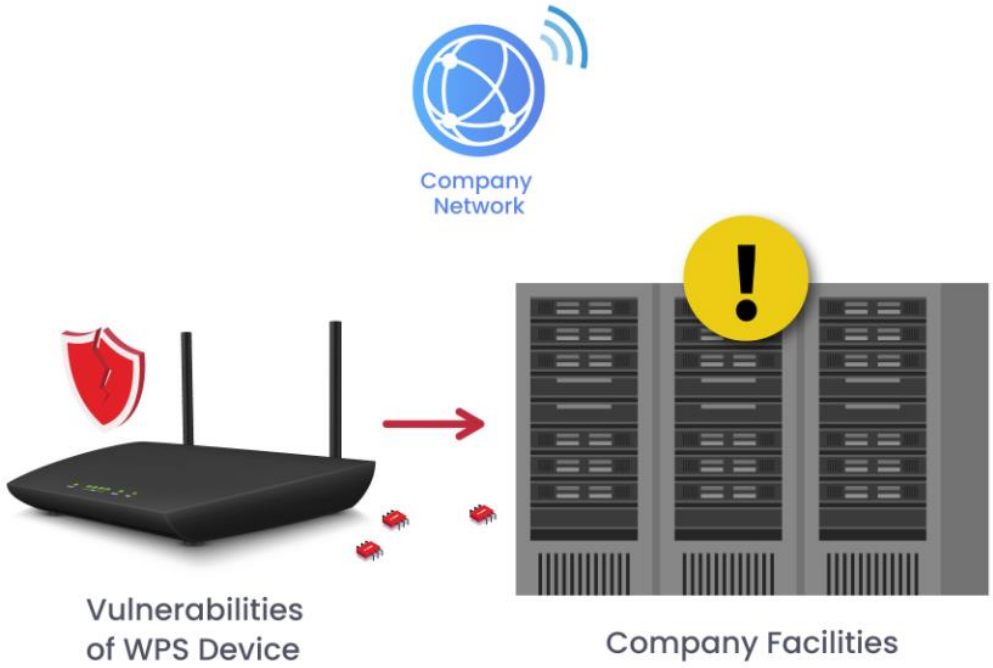


Abbildung 7: Schwachstellen von WPS können von Hackern ausgenutzt werden

Scannen

Tabelle 1 zeigt die Netzwerk-Ports, die häufig für Angriffe genutzt werden. Solange es keine IT-Kontrolle oder Überwachung gibt, werden solche Ports von Hackern als Einstiegspunkte für die Infiltration genutzt. Eine gängige Methode ist beispielsweise die Verwendung von Port-Scans, um Netzwerkteilnehmer im Unternehmen ausfindig zu machen, die Ports öffnen und dann diese Ports für schändliche Zwecke verwenden.

Port Number	*Service*	*Protocol(s)*
7	Echo	TCP, UDP
19	Chargen	TCP, UDP
20	FTP data (File Transfer Protocol)	TCP
21	FTP control	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Daytime	TCP, UDP
53	DNS (Domain Name System)	UDP
69	TFTP (Trivial File Transfer Protocol)	UDP
79	Finger	TCP, UDP
80	HTTP (Hypertext Transfer Protocol)	TCP
110	POP3 (Post Office Protocol version 3)	TCP
111	SUN RPC (remote procedure calls)	TCP, UDP
135	RPC/DCE (end point mapper) for Microsoft networks	TCP, UDP
137, 138, 139, 445	NetBIOS over TCP/IP	TCP, UDP
161	SNMP (Simple Network Management Protocol)	TCP, UDP
443	HTTPS (HTTP over SSL)	TCP
512, 513, 514	Berkeley r-services and r-commands (such as `rsh`, `rexec`, and `rlogin`)	TCP
1433	Microsoft SQL Server (ms-sql-s)	TCP, UDP
1434	Microsoft SQL Monitor (ms-sql-m)	TCP, UDP
1723	Microsoft PPTP VPN	TCP
3389	Windows Terminal Server	TCP
5631, 5632	pcAnywhere	TCP
8080	HTTP proxy	TCP

Tabelle 1: Häufig gehackte Ports

Abbildung 8: Windows Firewall MUSS Ports für Projektionssoftware öffnen zeigt, dass bei der Installation der drahtlosen Anwendung eines anderen Herstellers einige Netzwerkports in der Firewall des Benutzercomputers geöffnet werden müssen. Wenn diese Netzwerk-Ports im Unternehmensintranet nicht überwacht werden, stellen die nicht überwachten Netzwerk-Ports ein Risiko für das Unternehmensintranet dar.

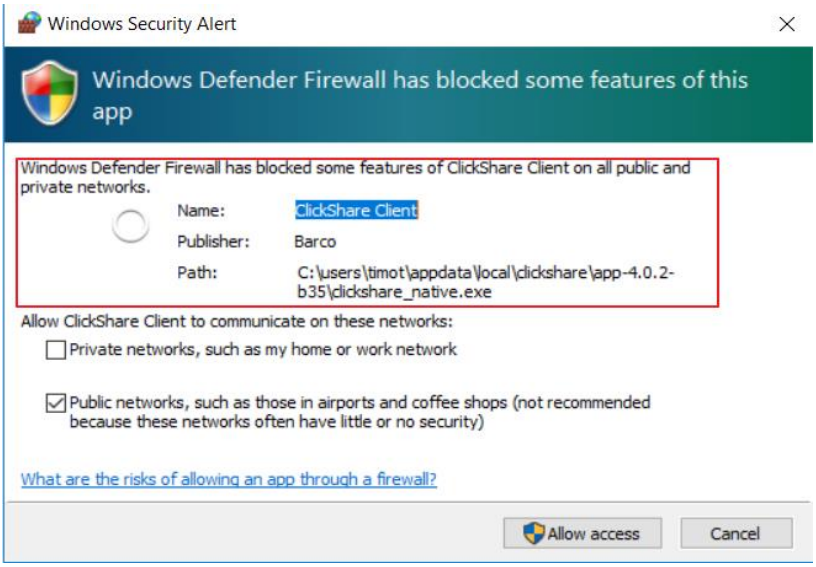
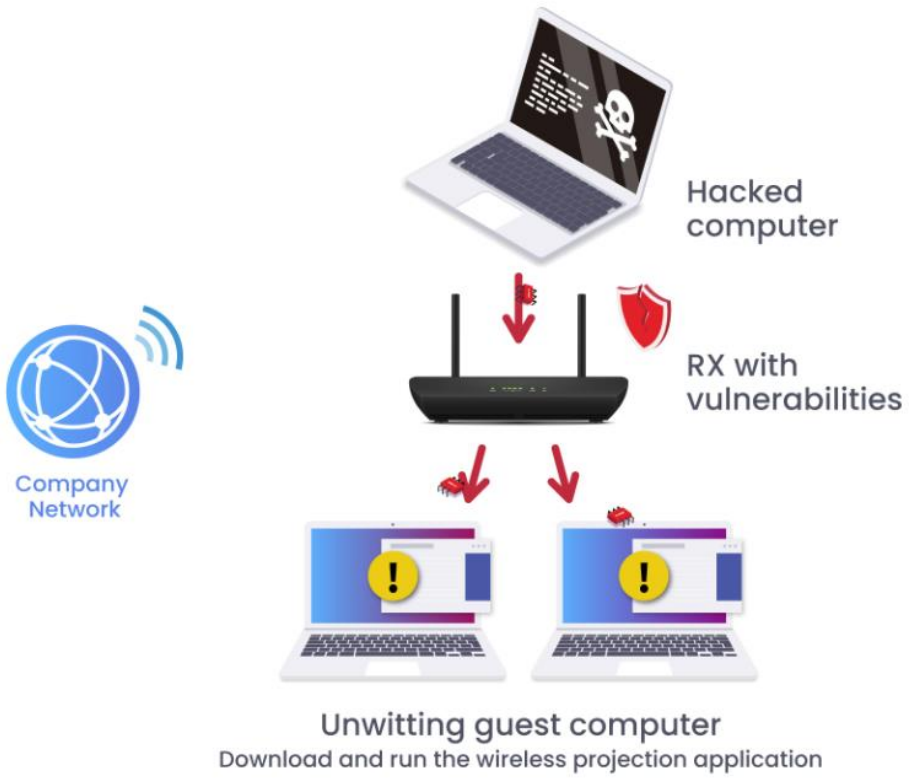


Abbildung 8: Windows Firewall MUSS Ports für Projektionssoftware öffnen

Scannen + Backdoor-Schadcode

In der Regel gibt es nicht nur eine Angriffsmethode; vielmehr ist es sehr wahrscheinlich, dass es sich um eine Mischung aus zwei oder mehr Angriffsarten handelt. Hier sind die 2 häufigsten Szenarien:

1. Wenn Hacker nach Schwachstellen im WPS-Empfänger suchen, können sie über das WAN des WPS-Empfängers in die Schwachstelle des Empfängers eindringen. Dann infizieren sie über den gekoppelten Sender den mit dem Sender verbundenen Computer und implantieren den schädlichen Backdoor-Code in den Sender-Computer. Wenn beispielsweise ein Besucher eine Präsentation halten muss, gibt das Unternehmen den Button des WPS-Senders an den Besucher weiter, damit dieser den Button direkt drücken kann, um seinen Bildschirm zu teilen. Wenn der gekoppelte Empfänger eine Sicherheitslücke aufweist, ist der Computer des Besuchers einem hohen Infektionsrisiko ausgesetzt. Wenn er unglücklicherweise infiziert ist, wird er beim nächsten Mal, wenn dieser Computer mit anderen Netzwerken verbunden wird, weiterhin andere Netzwerke infizieren.



2. Bei einigen WPS-Systemen muss ein Treiber für die App zur drahtlosen Projektion installiert werden, um die Funktion der Bildschirmprojektion nutzen zu können. Neben dem Risiko von Sicherheitsschwachstellen in der App selbst ist die App auch eine Brutstätte für das Einschleusen von Backdoor-Schadcode. In Abbildung 4 beispielsweise dringt der Hacker zunächst in das Unternehmensnetzwerk ein, dringt dann über den WPS-Empfänger und den gekoppelten Sender in den angeschlossenen Computer ein und implantiert dann den Backdoor-Schadcode in die WPS-App, um alle WPS-Bildschirmprojektionen aus der Ferne zu überwachen.

Über BenQ

Die BenQ Corporation wurde auf der Grundlage der Unternehmensvision "Bringing Enjoyment 'N' Quality to Life" gegründet und ist ein weltweit führender Anbieter von Humantechnologie und -lösungen mit dem Ziel, jeden Aspekt des Lebens der Verbraucher zu verbessern und zu bereichern. Um diese Vision zu verwirklichen, konzentriert sich das Unternehmen auf die Aspekte, die für die Menschen heute am wichtigsten sind - Lifestyle, Business, Gesundheit und Bildung - in der Hoffnung, den Menschen die Mittel an die Hand zu geben, um besser zu leben, die Effizienz zu steigern, sich gesünder zu fühlen und das Lernen zu verbessern. Zu diesen Mitteln gehört ein erfreulich breites Portfolio von Produkten und eingebetteten Technologien, die auf den Menschen ausgerichtet sind und digitale Projektoren, professionelle Monitore, interaktive großformatige Displays, Bildgebungslösungen, mobile Computer und LED-Beleuchtungslösungen umfassen. Because it matters.