Esempio di applicazione Microwall Gigabit:

Isolamento di una fresa CNC

Vai all'introduzione
Scheda tecnica Microwall

Per la produzione di prototipi e piccole serie la nostra azienda utilizza una fresa CNC. Sul computer di controllo, integrato nella nostra rete di produzione, è attivo Windows 7 standard incorporati a livello attuale del patch Dal momento che Microsoft nel 2020 interromperà il supporto ampliato per questo sistema operativo, questa fresa viene isolata a titolo preventivo. Con l'aiuto del router firewall "Microwall Gigabit" le viene assegnato un segmento di rete dedicato e la comunicazione con questo segmento di rete viene fortemente limitata tramite regole filtro.

Maggiore sicurezza della rete attraverso l'isolamento

Nel 2017 WannaCry si è fatto strada in tutto il mondo attraverso le reti e l'opinione pubblica mediatica. Il trojan criptafile ha sfruttato una vulnerabilità nell'abilitazione di file e stampanti delle reti Windows. Il suo effetto nocivo è stato così massiccio che Microsoft non solo ha dovuto rilasciare un patch per tutti i sistemi operativi attuali, ma ha dovuto fornire anche aggiornamenti di sicurezza per prodotti, già usciti dal supporto ampliato.

WannaCry ha mostrato in modo evidente, quali siano i potenziali di rischio che si generano dall'impiego di servizi di rete non necessari.

Sembra evidente la necessità di disattivare semplicemente i servizi superflui. Tuttavia non è sempre chiaro, quali servizi siano veramente necessari fra i vari componenti di un impianto. Inoltre eventuali modifiche alle macchine in alcuni casi possono determinare la perdita della certificazione e quindi il passaggio della responsabilità al gestore dell'impianto.

Per questo con il piccolo firewall Microwall Gigabit abbiamo sviluppato un'alternativa di facile uso per la protezione dei sistemi di produzione. In questo caso si tratta di un semplice firewall a 2 porte, che funziona secondo il principio whitelist. Ciò significa Che tutti i collegamenti ammessi devono essere esplicitamente abilitati.

Problema

La fresa è dotata di un computer di controllo Windows su cui è attivo il software CNC ed è dotato di due interfacce di rete. Una collega il computer con la fresa stessa, l'altra lo collega alla rete di produzione. Se si scopre una falla per la sicurezza nel sistema operativo allo stato attuale, si deve prevedere un aggiornamento tempestivo della sicurezza da parte di Microsoft. Al termine del supporto ampliato nel 2020, però, in genere non saranno più disponibili aggiornamenti di sicurezza. Un hacker potrebbe tentare di danneggiare il computer di controllo e, in caso di successo, il dispositivo stesso, ma anche la rete circostante sarebbero in pericolo.

Per questo motivo la fresa deve essere isolata utilizzando la strategia dell'isolamento. Con l'aiuto del Microwall Gigabit la fresa viene ricollocata in un segmento di rete dedicato e la comunicazione ammessa con questo segmento di rete viene fortemente limitata mediante regole del firewall.

Situazione di pericolo

Una breve analisi della situazione attuale con il port scanner nmap [Tutorial: Trovare porte aperte nella rete] evidenzia una realtà inquietante: Il computer di controllo mostra dodici porte aperte, raggiungibili attraverso la rete, fra cui anche un web server.

Una seconda scansione approfondita trova in totale 24 porte TCP aperte. Il webserver è un server di informazioni internet non configurato 7.5 che presenta noti punti deboli che possono determinare remote-code-execution. Ciò significa che un hacker potrebbe eseguire programmi a piacimento attraverso la rete. Una vincita al lotto per i cyberpirati. Dettaglio piccante: Il webserver sembra non fornire nient'altro di una pagina di informazioni, quindi è con tutta probabilità superfluo quanto le altre porte aperte. Siamo lieti di esserci presi il tempo per scansire in modo approfondito il sistema e avviare immediatamente l'isolamento.

Procedura

Fase 1: Determinazione del tipo di esercizio e delle regole firewall necessarie

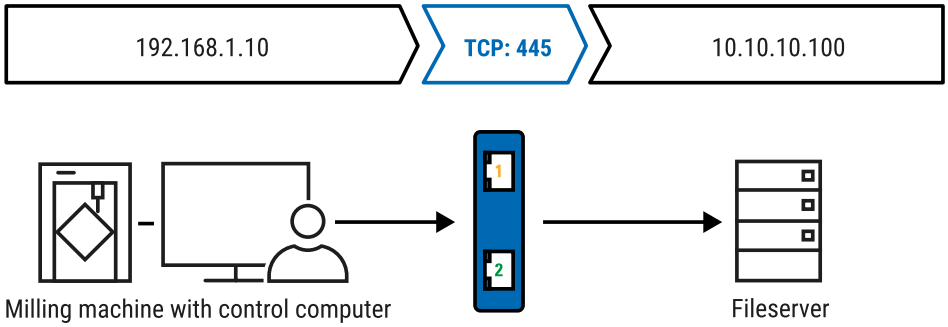
Per rendere la configurazione il più semplice possibile, gestiamo Microwall in modalità NAT. Il computer di controllo della fresa non compare neanche. Microwall si "mette nei suoi panni" per così dire, svolgendo le sue funzioni nella rete.

In realtà c'è solo un caso in cui la fresa deve comunicare attraverso la rete. Per poter accedere a dati di produzione, dovete poter stabilire un collegamento con il server di file centrale Windows. Tutti gli altri collegamenti vengono impediti.

Dal momento che il computer di controllo stesso non fornisce risorse nella rete, i collegamenti in entrata possono essere completamente bloccati. Inoltre l'abilitazione del server di file su cui dovrebbe avere accesso il software CNC è nota e chiara. Poiché l'indirizzo IP del file server è anch'esso noto, non è necessaria nessuna risoluzione del nome. Anche le funzioni comfort come la ricerca di computer e le abilitazioni attraverso la rete sono superflue, così come i protocolli di trasporto Netbios. Le porte 137, 138 e 139 possono dunque essere ignorate e quindi bloccate. Per aggiornamenti temporali automatici si potrebbe abilitare la porta UDP 123, per la risoluzione del nome tramite DNS la porta UPD 53. Dal momento che queste funzioni non sono necessarie per la funzione della fresa, anche queste rimangono chiuse.

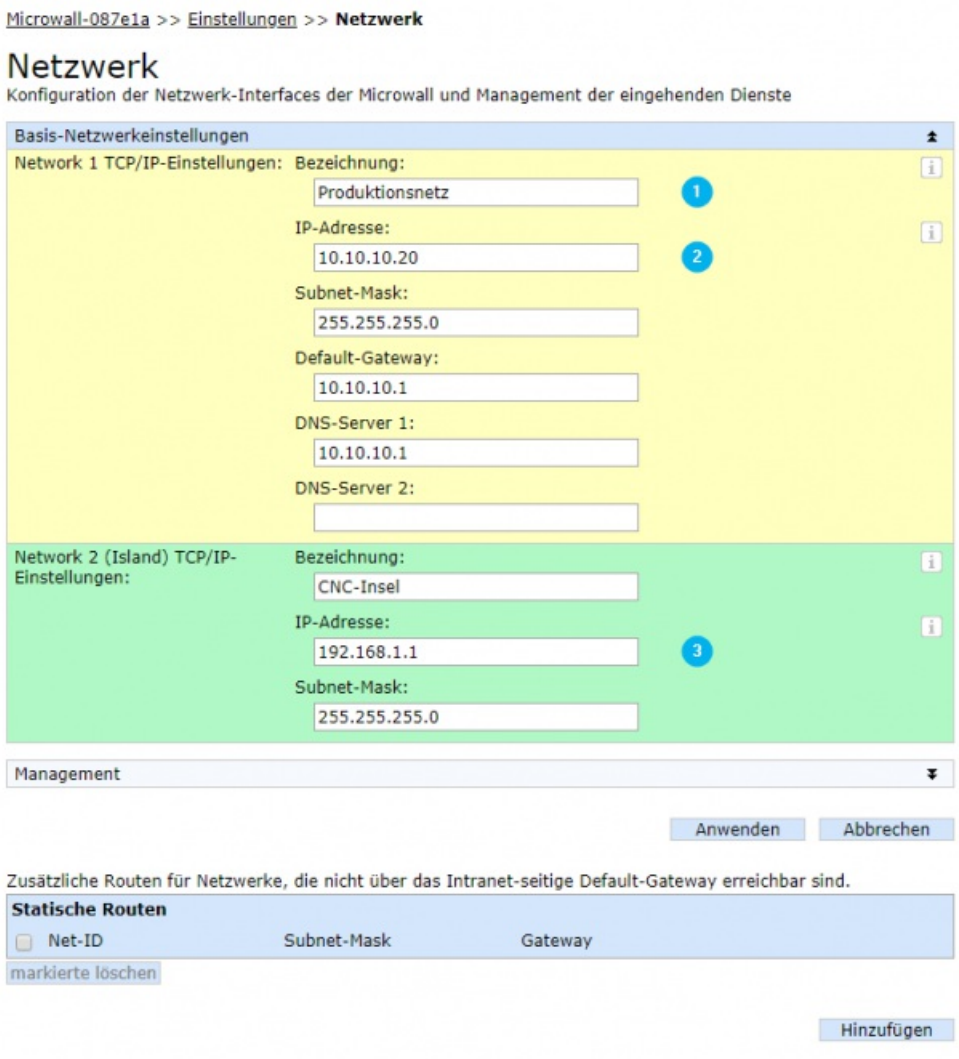
La gestione dei patch avviene attraverso il nostro reparto IT, per questo anche le porte rimangono chiuse per un aggiornamento automatico. Altrimenti dovrebbero consentire qui collegamenti TCP al server WSUS.

Il computer di controllo richiede solo la possibilità, di stabilire un collegamento SMB al file server con l'indirizzo IP conosciuto. Questo avviene attraverso la porta di destinazione 445. Poiché questa comunicazione avviene via TCP, il canale di ritorno è contenuto direttamente nel collegamento. **Con l'indicazione solo di una singola regola la fresa viene messa in sicurezza per un lungo periodo. Al contempo è garantita la sua funzione!**



Fase 2: Configurazione dell'apparecchio

Microwall, come router, unisce la rete circostante con un segmento isolato. Per le interfacce con entrambe le reti il Microwall ha bisogno rispettivamente di una configurazione IP.



1 L'indicazione di una denominazione di rete semplifica più tardi l'assegnazione di regole all'amministratore.

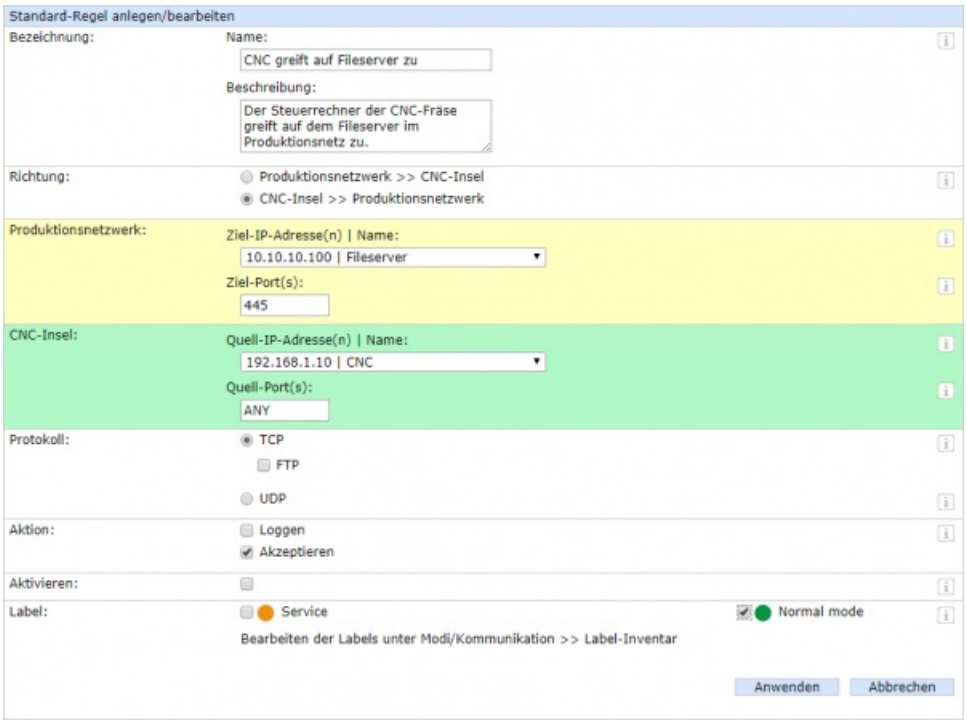
2 La configurazione IP iniziale del computer di controllo (ovvero 10.10.10.20) viene utilizzata per l'interfaccia pubblica.

Indipendentemente dall'indirizzo hardware nella rete circostante non cambia nulla.

3 Sul lato dell'isola scegliamo per semplicità la classica rete 192.168.1.0/24. Per questa rete Microwall funge da gateway standard e presenta l'indirizzo 192.168.1.1

Configurazione IP del computer di controllo
Al computer di controllo viene assegnato l'IP 192.168.1.10. Come gateway standard gli viene assegnato Microwall Gigabit con l'indirizzo IP 192.168.1.1.

Regola firewall per l'accesso al file server
Nell'ultimo passo impostiamo la necessaria regola firewall. Il computer di controllo con l'indirizzo IP 192.168.1.10 deve poter stabilire un collegamento TCP attraverso la porta 445 con il server dei dati di produzione con l'indirizzo IP 10.10.10.100.



Fase 3: Collaudo

Il collaudo che perdura ormai da alcune settimane dimostra che la fresa svolge il suo lavoro come sempre.

Sintesi

Con l'aiuto del Microwall la fresa CNC è stata isolata in soli pochi minuti in un segmento della rete proprio. Per garantire la funzione è stato sufficiente indicare una singola regola firewall. Come effetto secondario i protocolli NetBIOS per l'abilitazione del file e della stampante sono stati soppressi e quindi i dettagli sulla fresa sono stati nascosti dietro al Microwall.

Thomas Clever
t.clever@wut.de

Potete contattare telefonicamente i nostri tecnici al numero +49 202/2680-110 (Lun-Ven. 8-17)

W&T
www.WuT.de

Saremo lieti di fornirvi una consulenza personalizzata!

Wiesemann & Theis
GmbH
Porschestr. 12
42279 Wuppertal
Tel.: +49 202/2680-110 (Lun-Ven. 8-17)
Fax: +49 202/2680-265
info@wut.de