Technical University of Delft
Drops Nessus
And Dramatically Reduces
Network Security Man-Hours

Are you considering adding more restrictions to your users to reduce security headaches?

Here's how a university with 15,000 students keeps its network secure enough to satisfy the demands of the tech industries and governments that support research and open enough to satisfy the students!

Technical University of Delft
Location: Delft, Netherlands

Founded: 1842 by King Willem II

Business: Netherland's largest technical university

Business Units: Multi-location Campus, 6,000 staff, 5,000 student rooms and 15,000 laptop wielding students from around the world

Recipe for Success: TU Delft is known for its high standards in research and education. TU Delft has many contacts with governments, trade, consultancy programs, industry and SMEs.

Introduction

Established in 1842, and located in Delft, in the Netherlands, the Technical University of Delft's (TU Delft) is the nation's largest technical university, with a network that supports some 6,000 staff and around 15,000 students. To secure their network, the university uses central solutions such as anti-virus and anti-spam, But there are other hazards, such as the dangers involved in visiting risky websites, and active hacking attempts to exploit specific vulnerabilities. To manage these risks, TU Delft now uses the AVDS scanning appliance from Beyond Security.

The Challenge

To prevent the possibility of infections and attempted hacking, TU Delft uses scanning systems which check the network's vulnerable components. The scanner TU Delft used had reached the end of its life-cycle. It required considerable management and had a difficult to use interface. This was the starting point for the search for a new scanning system which would be easy to manage, reliable and user-friendly.

Solution

Security partner Pinewood implemented the AVDS scanning appliance from Beyond Security.

Benefits

With the AVDS scanning appliance from Beyond Security, TU Delft has largely automated the scanning process. At the same time the results and reports offer valuable insights for concrete security measures. The clear user interface also contributes substantially to user-friendliness and a flexible deployment of the solution. An extra benefit is that this is a hardened appliance which requires no extra management. With AVDS, TU Delft has more control of their network, and an insight into, the risks threatening their network.

TU Delft Strengthens its Grip on Vulnerabilities with Beyond Security

Network protection is a high priority at the Technical University of Delft. In addition to some 6,000 staff and around 15,000 students, the network supports the university's various locations, including some 5,000 connected student rooms. Securing the network is tackled at a variety of levels. The central security solution for anti-virus and anti-spam blocks the majority of the viruses and spam messages. But danger also lurks in other areas.

"We now have the ability to scan at any time. Regular vulnerability assessments scans are like having sonar on our own network. We always know what is going on around us."
–Mike Gutknecht
Network Engineer
Rayovac Corporation

There are considerable dangers associated with visiting risky websites and active hacking attempts targeting specific vulnerabilities. To also be able to get to grips with these risks, TU Delft now uses the AVDS scanning appliance from Beyond Security, which scans the network for vulnerabilities. This process is fully automated, and the results offer valuable insights for concrete security measures.

"Within TU Delft, we have worked on a constructive security policy for our network, including monitoring, for years. Alongside technical, organizational and physical measures against risks such as viruses, spam, phishing and other threats, we also work hard at strengthening awareness in terms of security," explains Alf Moens, Information Security Manager with TU Delft. "We certainly have got to grips with securing the network itself. We have had few instances of viruses over the past two years, for example, while also managing to block 95 per cent of incoming spam. The greatest risk lies with the users. For example, each year we take in thousands of new students, including from abroad. And they want to make maximum use of our broadband network. There are certainly risks attached to this too."

Peer-to-peer websites

One of the risks is that TU Delft currently has little ability to check whether external network users’ equipment have up-to-date security software installed. Add this to the fact that it is difficult to influence the conduct of internet users. Most infections actually arise from visits to risky websites which install malware, spyware or phishing tools surreptitiously. Peer-to-peer sites also constitute a major risk. And not only through problems arising from downloading and particularly also distributing material which is subject to copyright.

It is in fact also difficult to determine whether dangerous software or other tools are hitching a ride with the data users are accessing. But at the same time Moens has no intentions of blocking access to these applications. “Peer-to-peer tools are used extensively within our organization to exchange scientific data. Here they support a core activity of our organization. This does however mean that we must carefully monitor traffic on the network and the potential vulnerabilities.”

Replacing Nessus

To avoid the possibility of infections and hacking attempts, TU Delft has for some time been using scanning systems which check the vulnerable components of the network. The scanner seeks out vulnerable systems and servers on the network. This will happen on an up-to-date database which alerts us to the most common vulnerabilities. For example, when a system has not had the latest patches installed. If this is the case, it will be reported and the administrator can take appropriate action.

For scanning vulnerabilities TU Delft used the semi-open-source tool Nessus. Moens: “The scanning results of this solution are good, but using the solution requires specialist technical knowledge. It is also difficult to get support for specific components. Because it’s an open-source solution we have to look for that ourselves. Another restricting factor is the fact that it does not have a user-friendly interface. This makes deploying the system extremely labor-intensive in an extensive network such as ours, which influences the costs. It’s also difficult to scan specific systems or network components. And the system itself requires a great deal of administrative activity. All in all the Nessus system had reached the end of its lifecycle for us.”

AVDS graphically, unobtrusively and with great detail demonstrated to me the situation of our network/firewall and web server after scanning our system with a huge range of tests. Reports were sent to me that were concise and clear and then the technical staff of Beyond Security talked me through the results of the scans, interpreting areas with which I was unfamiliar and suggesting simple and precise fixes. From the moment of my first contact with Beyond Security, I have been impressed and enjoyed their friendliness, clear talking, approach to confidentiality and technical knowledge.”
–Paul Sheriff
IT Manager
City of Geraldton

Practical tests

During the search for a new scanning solution, Moens was referred to the AVDS scanning appliance from Beyond Security by a Security Manager from another university. “His experiences were very positive and was a sufficient reason to carry out a practical test..” The accessibility and manageability of Beyond Security turned out to be a strong point. The ease of use and simplicity of the user interface made it very easy to work with. Another advantage is that it is a hardened appliance. This means no extra management is needed, as with Nessus which runs on a separate Linux machine.” After the decision was made, security specialist Pinewood was drafted in. “We have worked many times with Pinewood in the past. These professionals have considerable expertise when it comes to security. Pinewood is our central reference point. Their offices are close to the university. This makes it possible to link up quickly. They supervised the installation and provided brief instruction via on-the-job training. The solution’s user-friendly setup actually did the rest.”

Ad hoc scans

Initially TU Delft is deploying Beyond Security for the weekly VLAN scans. These scans will be fully automated, and run in the background. Intervention will only be needed if something is actually detected. At the same time the new solution will be used for ad-hoc scanning. Moens: “For the time being Nessus will remain operational for specific scanning tasks. We are going to use the flexibility of the Beyond Security solution for the ad hoc scans we carry out for special events. Thus spikes in mail traffic could indicate that a computer has been taken over and is being misused for sending out spam. Or a vulnerability might occur. At such a time the Computer Emergency Response Team (TUD-CERT) will be drafted in. The deployment of Beyond Security accelerates the speed and strength of this team. They can indicate via a web interface which IP addresses need to be checked. The GUI of Beyond Security simplifies this scanning process.”

Measurability

Moens also regards the Beyond Security reports as a big plus. “The well-organized scanning reports make it possible to analyze vulnerability data historically. We can deploy automatic trend analyses for this. Thus it is relatively easy to follow the development of various vulnerabilities. We can then use this knowledge to protect our network even better against risks.”

The information provided in the reports is very clear and concise. It explains to engineers what the problem is, where to look for more information, and how to fix it. “With these reports we can be sure after every change to the network if we are making the right change in terms of our security requirements.
“We tried the free services. But when we piloted AVDS, we saw zero false positives and the differential reports make Management Reporting easy. These features are huge. They allow us to focus on delivering ICT services instead of chasing down vulnerabilities.”
–Cody Phang
Head of IT for the Australian Government National Capital Authority (NCA)

The choice for Beyond Security also fits within a broader development of IT management within TU Delft. “With the IT division we are striving towards the introduction of an integrated management system. At the same time the administrator has integrated responsibility over his own domain. This encompasses aspects such as capacity management, the concern that a system remains operational. Resolving problems such as vulnerabilities is also part of this. However this requires an insight into the vulnerabilities, so that the latest patches have always been installed. Choosing Beyond Security is yet another step in further professionalizing our IT department. By scanning very frequently, and where possible automatically, administrators have quick and easy access to relevant information to protect their network domain or systems to the maximum.”

Contact Information

USA
1616 Anderson Road
McLean, VA 22102
+1 800 801 2821
aviram@beyondsecurity.com

19925 Stevens Creek Blvd.
Cupertino, CA 95014
+1 408 329-6041
donw@beyondsecurity.com

EMEA
105 London St. Suite 609
Reading RG1 4QD
UK
+44 203 006 3022
zvim@beyondsecurity.com

Asia Pacific
Post Office Box 4
Mount Colah NSW 2079
Australia
+61 401 778 124
steveh@beyondscurity.com

China
5/F South Block Tower C,
Rathcom Info Tech Park,
No 2 Kexueyuan South Rd.
Haidian District Beijing 100190
+86 10 598 22211
thomasz@beyondsecurity.com