# Table of Contents

Grundlegende Informationen und Methodologie ............................................. 2

Zusammenfassung ......................................................................................... 3
  Sicherheit und Bedrohungsabwehr .......................................................... 3
  Applikationskategorien .......................................................................... 3

Empfohlene Maßnahmen ............................................................................ 4

Sicherheit und Bedrohungsabwehr ............................................................... 5
  Definition Applikationsrisiko ................................................................ 5
  Risikobehaftete Applikationskategorien .............................................. 6
  Angriffe ................................................................................................. 7
  Erkannte Angriffe .................................................................................. 7
  Angriffsziele .......................................................................................... 7
  Angriffsquellen ...................................................................................... 8
  Malware, Botnetze, Spyware/Adware ...................................................... 8
  Erkannte Malware .................................................................................. 8
  Malware Ziele ........................................................................................ 8
  Malware Quellen .................................................................................... 8
  Erkannte Botnetze .................................................................................. 9
  Botnet Ziele ........................................................................................... 9
  Botnet Quellen ....................................................................................... 9
  Gefährdete Nutzer und Geräte ............................................................... 10
  Top Geräte nach Reputation Scores ...................................................... 10

Nutzerproduktivität ...................................................................................... 11
  Verhältnis HTTPS zu HTTP ................................................................. 11
  HTTP SSL Ratio .................................................................................... 11
  Top Zielländer nach Zeit ....................................................................... 11
  Top-Cloud-Anwendungen .................................................................. 12
  Top-Fernzugriffsanwendungen ............................................................ 12
  Top-Proxy-Anwendungen ..................................................................... 12
  Top-Social-Media-Anwendungen ......................................................... 13
  Top-Video-/Audio-Streaming-Anwendungen ......................................... 14
  Top-Spieleanwendungen ....................................................................... 14
  Top-Peer-to-Peer-Anwendungen .......................................................... 14

Webnutzung .................................................................................................. 15
  Top-Webkategorien .............................................................................. 15
  Top-Webanwendungen ......................................................................... 15
  Meist besuchte Webdomänen .............................................................. 16
  Meist besuchte Webdomänen nach Surfzeit ........................................ 17

Netzwerknutzung ....................................................................................... 18
  Bandbreitenerschöpfende Top-Quellen/-Ziele ...................................... 18
  Übersicht über das Sessionaufkommen während des ECTAS ............... 19
  Aktive Benutzer .................................................................................... 19

Appendix A .................................................................................................. 20
  Devices ................................................................................................. 20
Grundlegende Informationen und Methodologie


Der Report wurde aufgrund folgender Charakteristiken erstellt:

**Firmendetails**

- **Firmenname**: ACME Inc.
- **Standort**: Münster
- **Branche**: Handel
- **Firmengröße**: 300 Mitarbeiter

**Details der Messung**

- **Startdatum**: DD.MM.YYYY  
  **Enddatum**: DD.MM.YYY
- **Analyse Equipment**: ECTA-300D  
  **Analyse Version**: 5.4.1
- **Analysiertes Netzwerk**: Produktionsnetzwerk  
  **Bemerkung**:

**Aufbau und Methode der Messung**

Ihr Netzwerk-Datenverkehr wurde mit einer ECTA-300D analysiert. Dazu wurden der Analyseappliance über einen SPAN-Port Ihrer Switch-Infrastruktur die nötigen Daten zur Verfügung gestellt. Die Analyse fand am Perimeter-Gateway statt, d.h. es wurde der ein- und ausgehende Datenverkehr vor Ihrer Firewall (vom internen Netz aus betrachtet) analysiert.


Zusammenfassung

Sicherheit und Bedrohungabwehr

- Malicious & Phishing Sites: 54
- Critical & High Intrusion Attack: 8
- Malware & Botnet C&C: 4

66 Threat

Applikationskategorien

Empfohlene Maßnahmen

Botnet und Malware Infektionen: 63


Tunnel Applikationen: 3

Proxy- oder Tunnelapplikationen werden häufig genutzt um existierende Sicherheitsmaßnahmen zu umgehen. Dies hat Auswirkungen auf Ihr Unternehmen sowie auf die Sicherheit. Entsprechende Sicherheitsregeln auf Firewalls und interne Policies, die die Nutzung solcher Applikationen regeln sollten implementiert werden.

P2P Applikationen: 2


Stark bandbreitenintensive Applikationen: 65

Bandbreitenintensive Applikationen können den normalen Geschäftsablauf und die Performance der unternehmenskritischen Anwendungen negativ beeinflussen. Entsprechende Regeln auf dem Perimeter sollten evaluiert werden. Dazu zählen zeitliche Beschränkungen, komplette Sperrungen aber auch Bandbreiteneinschränkungen durch QoS.
Sicherheit und Bedrohungsabwehr
Definition Applikationsrisiko

Applikationen wird basierend auf ihrem Verhalten und den möglichen Auswirkungen eine Risikobewertung von 1 bis 5 zugewiesen. Diese Unterteilung erlaubt es Administratoren risikobehaftete Applikationen schnell zu erkennen und Reports entsprechend zu strukturieren.

<table>
<thead>
<tr>
<th>Risikobewertung</th>
<th>Charakteristisches Verhalten</th>
<th>Beispiele</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Kritisch</td>
<td>Bösartige Applikationen oder solche, die dazu genutzt werden können, diverse Sicherheitsmaßnahmen zu umgehen.</td>
<td>Botnet oder Proxy Applikationen</td>
</tr>
<tr>
<td>4 Hoch</td>
<td>Applikationen, die Malwareinfektionen oder &quot;Data Leakage&quot; verursachen können. Solche Applikationen sind häufig persönliche / private file-sharing Applikationen oder solche, die Datenverkehr tunneln um Sicherheitsmaßnahmen zu umgehen.</td>
<td>P2P oder Remote Access Applikationen</td>
</tr>
<tr>
<td>3 Erhöht</td>
<td>Applikationen, die der persönlichen / privaten Kommunikation dienen oder bekannte Schwachstellen haben.</td>
<td>IM, Email, Storage oder Backup Applikationen</td>
</tr>
<tr>
<td>2 Überwacht</td>
<td>Applikationen, die oft eine erhöhte Bandbreitenutzung nach sich ziehen oder die Effektivität beeinflussen können.</td>
<td>Spiele, Social Media, Video/Audio Applikationen</td>
</tr>
<tr>
<td>1 Niedrig</td>
<td>Geschäftliche Applikationen oder Software Update Mechanismen.</td>
<td>Update oder Business Applikationen</td>
</tr>
</tbody>
</table>
Risikobehaftete Applikationskategorien

Bei der Messung in Ihrem Netzwerk wurden folgende potentiell risikobehaftete Applikationskategorien ermittelt:

- Remote.Access: 8
- Proxy: 7
- P2P: 2
- Botnet: 1

<table>
<thead>
<tr>
<th>#</th>
<th>Risiko</th>
<th>Applikation</th>
<th>Kategorie</th>
<th>Technologie</th>
<th>Benutzer</th>
<th>Bandbreite</th>
<th>Verbindungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>Proxy.HTTP</td>
<td>Proxy</td>
<td>Network-Protocol</td>
<td>21</td>
<td>11.55 MB</td>
<td>857</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>Tor</td>
<td>Proxy</td>
<td>Client-Server</td>
<td>1</td>
<td>5.36 MB</td>
<td>86</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>Zeroaccess.Botnet</td>
<td>Botnet</td>
<td>Client-Server</td>
<td>1</td>
<td>864 B</td>
<td>54</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>Peer2me</td>
<td>Proxy</td>
<td>Client-Server</td>
<td>1</td>
<td>1.17 MB</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>OK1HTTP.Library,VPN</td>
<td>Proxy</td>
<td>Client-Server</td>
<td>1</td>
<td>5.74 KB</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>Tor2web</td>
<td>Proxy</td>
<td>Browser-Based</td>
<td>1</td>
<td>483 B</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>SOCKS4</td>
<td>Proxy</td>
<td>Network-Protocol</td>
<td>1</td>
<td>28 B</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>DNS,TXT,Records,Tunneling</td>
<td>Proxy</td>
<td>Client-Server</td>
<td>1</td>
<td>11.87 KB</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>AnyDesk</td>
<td>Remote.Access</td>
<td>Client-Server</td>
<td>48</td>
<td>613.15 MB</td>
<td>157,851</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>TeamViewer</td>
<td>Remote.Access</td>
<td>Client-Server</td>
<td>48</td>
<td>115.53 MB</td>
<td>9,786</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>Citrix.Receiver</td>
<td>Remote.Access</td>
<td>Client-Server</td>
<td>31</td>
<td>84.25 MB</td>
<td>8,497</td>
</tr>
<tr>
<td>12</td>
<td>4</td>
<td>RDP</td>
<td>Remote.Access</td>
<td>Client-Server</td>
<td>17</td>
<td>25.29 MB</td>
<td>209</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>BitTorrent,HTTP,Seed</td>
<td>P2P</td>
<td>Peer-to-Peer</td>
<td>23</td>
<td>2.53 KB</td>
<td>162</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
<td>TeamViewer_CallRequesst</td>
<td>Remote.Access</td>
<td>Client-Server</td>
<td>14</td>
<td>254.73 MB</td>
<td>117</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>BitTorrent</td>
<td></td>
<td></td>
<td>59</td>
<td>6.71 KB</td>
<td>77</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>TeamViewer_CallReceiv e</td>
<td>Remote.Access</td>
<td>Client-Server</td>
<td>5</td>
<td>17.18 MB</td>
<td>14</td>
</tr>
<tr>
<td>17</td>
<td>4</td>
<td>VNC</td>
<td>Remote.Access</td>
<td>Client-Server</td>
<td>2</td>
<td>5.78 MB</td>
<td>11</td>
</tr>
<tr>
<td>18</td>
<td>4</td>
<td>MS.Netlogon</td>
<td>Remote.Access</td>
<td>Client-Server</td>
<td>4</td>
<td>36.69 KB</td>
<td>6</td>
</tr>
</tbody>
</table>
Angriffe

Erkannte Angriffe

<table>
<thead>
<tr>
<th>#</th>
<th>Attack Name</th>
<th>Severity</th>
<th>CVE-ID</th>
<th>Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Obfuscated.Flash.Exploit</td>
<td>Critical</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Sundown.Exploit.Kit</td>
<td>Critical</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>IP.Bad.Header</td>
<td>Critical</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>Worm.Slammer</td>
<td>high</td>
<td>CVE-2002-0649</td>
<td>387</td>
</tr>
<tr>
<td>9</td>
<td>BlackNurse.ICMP.Type.3.Code.e.3.Flood.DoS</td>
<td>medium</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>SIP.Vicious.SIP.Scanner</td>
<td>low</td>
<td></td>
<td>717</td>
</tr>
<tr>
<td>11</td>
<td>PHP.Remote.File.Inclusion</td>
<td>low</td>
<td></td>
<td>246</td>
</tr>
<tr>
<td>12</td>
<td>Port.Scanning</td>
<td>low</td>
<td></td>
<td>11</td>
</tr>
</tbody>
</table>

Angriffziele

<table>
<thead>
<tr>
<th>#</th>
<th>Attack Victim</th>
<th>Counts</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Percent of Total Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>78</td>
<td>6.86%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>76</td>
<td>6.68%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>75</td>
<td>6.60%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>74</td>
<td>6.51%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>73</td>
<td>6.42%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>72</td>
<td>6.33%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>71</td>
<td>6.24%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>70</td>
<td>6.16%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td>70</td>
<td>6.16%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>de</td>
<td></td>
<td>69</td>
<td>6.07%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>69</td>
<td>6.07%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td>68</td>
<td>5.98%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td>67</td>
<td>5.89%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td>64</td>
<td>5.63%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td>63</td>
<td>5.54%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td>3</td>
<td>0.26%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td>3</td>
<td>0.26%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td>1</td>
<td>0.09%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td>1</td>
<td>0.09%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td>1</td>
<td>0.09%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Angriffsquellen

<table>
<thead>
<tr>
<th>#</th>
<th>Attack Source</th>
<th>Counts</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Percent of Total Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>245</td>
<td>76</td>
<td>136</td>
<td>33</td>
<td>28.76%</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>87</td>
<td>1</td>
<td>77</td>
<td>3</td>
<td>10.21%</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>64</td>
<td>49</td>
<td>2</td>
<td>7</td>
<td>7.61%</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>64</td>
<td>49</td>
<td>2</td>
<td>7</td>
<td>7.61%</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>45</td>
<td>26</td>
<td>2</td>
<td>7</td>
<td>5.28%</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>33</td>
<td>14</td>
<td>5</td>
<td>4</td>
<td>3.76%</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>32</td>
<td>14</td>
<td>5</td>
<td>4</td>
<td>3.76%</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>32</td>
<td>14</td>
<td>5</td>
<td>4</td>
<td>3.76%</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>32</td>
<td>14</td>
<td>5</td>
<td>4</td>
<td>3.76%</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>32</td>
<td>14</td>
<td>5</td>
<td>4</td>
<td>3.76%</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>30</td>
<td>11</td>
<td>6</td>
<td>3</td>
<td>3.52%</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>24</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td>2.82%</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>19</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td>2.23%</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>18</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td>2.11%</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>17</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td>2.00%</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>17</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td>2.00%</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>17</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td>2.00%</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>16</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td>1.88%</td>
</tr>
<tr>
<td>19</td>
<td></td>
<td>14</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td>1.64%</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>14</td>
<td>5</td>
<td>15</td>
<td>4</td>
<td>1.64%</td>
</tr>
</tbody>
</table>

### Malware, Botnetze, Spyware/Adware

#### Erkannte Malware

<table>
<thead>
<tr>
<th>#</th>
<th>Malware Name</th>
<th>Malware Type</th>
<th>Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EICAR_TEST_FILE</td>
<td>Virus</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>JS/IFRAME.CNTltr</td>
<td>Virus</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>W32/Kryptik.FSBIntr</td>
<td>Virus</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Malware Ziele

<table>
<thead>
<tr>
<th>#</th>
<th>Victim Name (or IP)</th>
<th>Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IPv4-39156</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>IPv4-28266</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>IPv4-51756</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Malware Quellen

<table>
<thead>
<tr>
<th>#</th>
<th>Malware Source</th>
<th>Hostname (or IP)</th>
<th>Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IPv4-39156</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>IPv4-28266</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>IPv4-51756</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
Erkannte Botnetze

<table>
<thead>
<tr>
<th>Botnet Name</th>
<th>Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zeroaccess.Botnet</td>
<td>54</td>
</tr>
</tbody>
</table>

Botnet Ziele

<table>
<thead>
<tr>
<th>Victim Name (or IP)</th>
<th>Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4-33281</td>
<td>54</td>
</tr>
</tbody>
</table>

Botnet Quellen

<table>
<thead>
<tr>
<th>C&amp;C IP</th>
<th>Hostname</th>
<th>Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4-23257</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>IPv4-27544</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>IPv4-53995</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>IPv4-23310</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>IPv4-52772</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>IPv4-40640</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>IPv4-27215</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IPv4-58147</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IPv4-65202</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IPv4-53114</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IPv4-54197</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IPv4-2915</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IPv4-57981</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IPv4-65516</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IPv4-15349</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>IPv4-44630</td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>
Gefährdete Nutzer und Geräte


<table>
<thead>
<tr>
<th>#</th>
<th>Device</th>
<th>Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>35,975</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>8,735</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>7,320</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>6,450</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>5,940</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>5,580</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>4,975</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>4,740</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>4,330</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>3,690</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>3,200</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>3,200</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>2,700</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>2,610</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>2,460</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>2,360</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>2,300</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>2,250</td>
</tr>
<tr>
<td>19</td>
<td></td>
<td>2,220</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>2,210</td>
</tr>
</tbody>
</table>
Nutzerproduktivität

Verhältnis HTTPS zu HTTP
HTTP SSL Ratio

63.09% HTTPS (303.76 GB)
36.91% HTTP (177.73 GB)

Top Zielländer nach Zeit

<table>
<thead>
<tr>
<th>#</th>
<th>Destination</th>
<th>Browsing Time (hh:mm:ss)</th>
<th>Bandwidth</th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United Kingdom</td>
<td>332:20:01</td>
<td></td>
<td>1.12 GB</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>United States</td>
<td>241:26:06</td>
<td></td>
<td>58.27 GB</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Ireland</td>
<td>217:22:23</td>
<td></td>
<td>2.61 GB</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Netherlands</td>
<td>210:42:17</td>
<td></td>
<td>5.68 GB</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Germany</td>
<td>158:40:59</td>
<td></td>
<td>13.62 GB</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>France</td>
<td>29:05:51</td>
<td></td>
<td>651.17 MB</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Canada</td>
<td>09:26:05</td>
<td></td>
<td>829.15 MB</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>China</td>
<td>04:20:58</td>
<td></td>
<td>21.95 MB</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Czech Republic</td>
<td>04:09:56</td>
<td></td>
<td>105.54 MB</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Japan</td>
<td>03:47:31</td>
<td></td>
<td>16.92 MB</td>
<td></td>
</tr>
</tbody>
</table>
### Top-Cloud-Anwendungen

<table>
<thead>
<tr>
<th>#</th>
<th>Application</th>
<th>Action</th>
<th>Bandwidth</th>
<th>Session Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Amazon.AWS.S3</td>
<td>Allowed</td>
<td>404.73 MB</td>
<td>6,611</td>
</tr>
<tr>
<td>2</td>
<td>Amazon.AWS</td>
<td>Allowed</td>
<td>369.84 MB</td>
<td>3,234</td>
</tr>
<tr>
<td>3</td>
<td>Fortiguard.Search</td>
<td>Allowed</td>
<td>121.45 MB</td>
<td>1,975,690</td>
</tr>
<tr>
<td>4</td>
<td>Microsoft.Azure</td>
<td>Allowed</td>
<td>31.37 MB</td>
<td>4,269</td>
</tr>
<tr>
<td>5</td>
<td>Godaddy</td>
<td>Allowed</td>
<td>18.73 MB</td>
<td>7,276</td>
</tr>
<tr>
<td>6</td>
<td>TrendMicro.WFBS</td>
<td>Allowed</td>
<td>1.06 MB</td>
<td>23</td>
</tr>
<tr>
<td>7</td>
<td>Google.Cloud.Platform</td>
<td>Allowed</td>
<td>585.12 KB</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>Twilio</td>
<td>Allowed</td>
<td>51.75 KB</td>
<td>1</td>
</tr>
</tbody>
</table>

### Top-Fernzugriffsanwendungen

<table>
<thead>
<tr>
<th>#</th>
<th>Application</th>
<th>Action</th>
<th>Bandwidth</th>
<th>Session Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AnyDesk</td>
<td>Allowed</td>
<td>613.15 MB</td>
<td>157,851</td>
</tr>
<tr>
<td>2</td>
<td>TeamViewer_CallRequest</td>
<td>Allowed</td>
<td>254.73 MB</td>
<td>117</td>
</tr>
<tr>
<td>3</td>
<td>TeamViewer</td>
<td>Allowed</td>
<td>115.53 MB</td>
<td>9,786</td>
</tr>
<tr>
<td>4</td>
<td>Citrix.Receive</td>
<td>Allowed</td>
<td>84.25 MB</td>
<td>8,497</td>
</tr>
<tr>
<td>5</td>
<td>RDP</td>
<td>Allowed</td>
<td>25.29 MB</td>
<td>209</td>
</tr>
<tr>
<td>6</td>
<td>TeamViewer_CallReceive</td>
<td>Allowed</td>
<td>17.18 MB</td>
<td>14</td>
</tr>
<tr>
<td>7</td>
<td>VNC</td>
<td>Allowed</td>
<td>5.78 MB</td>
<td>11</td>
</tr>
<tr>
<td>8</td>
<td>MS.Netlogon</td>
<td>Allowed</td>
<td>36.69 KB</td>
<td>6</td>
</tr>
</tbody>
</table>

### Top-Proxy-Anwendungen

<table>
<thead>
<tr>
<th>#</th>
<th>Application</th>
<th>Action</th>
<th>Bandwidth</th>
<th>Session Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Proxy,HTTP</td>
<td>Allowed</td>
<td>11.55 MB</td>
<td>857</td>
</tr>
<tr>
<td>2</td>
<td>Tor</td>
<td>Allowed</td>
<td>5.36 MB</td>
<td>86</td>
</tr>
<tr>
<td>3</td>
<td>Peer2me</td>
<td>Allowed</td>
<td>1.17 MB</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>OpenVPN</td>
<td>Allowed</td>
<td>1.16 MB</td>
<td>22</td>
</tr>
<tr>
<td>5</td>
<td>PPTP</td>
<td>Allowed</td>
<td>483.90 KB</td>
<td>558</td>
</tr>
<tr>
<td>6</td>
<td>L2TP</td>
<td>Allowed</td>
<td>45.25 KB</td>
<td>433</td>
</tr>
<tr>
<td>7</td>
<td>DNS.TXT,Records.Tunneling</td>
<td>Allowed</td>
<td>11.87 KB</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>OKHTTP,Library,VPN</td>
<td>Allowed</td>
<td>5.74 KB</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>Tor2web</td>
<td>Allowed</td>
<td>483 B</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>SOCKS4</td>
<td>Allowed</td>
<td>28 B</td>
<td>2</td>
</tr>
</tbody>
</table>
### Top-Social-Media-Anwendungen

<table>
<thead>
<tr>
<th>#</th>
<th>Application</th>
<th>Action</th>
<th>Bandwidth</th>
<th>Session Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Facebook</td>
<td>Allowed</td>
<td>10.70 GB</td>
<td>84,854</td>
</tr>
<tr>
<td>2</td>
<td>Instagram</td>
<td>Allowed</td>
<td>6.15 GB</td>
<td>12,186</td>
</tr>
<tr>
<td>3</td>
<td>Tumblr</td>
<td>Allowed</td>
<td>1.90 GB</td>
<td>6,299</td>
</tr>
<tr>
<td>4</td>
<td>Twitter</td>
<td>Allowed</td>
<td>1.67 GB</td>
<td>22,010</td>
</tr>
<tr>
<td>5</td>
<td>DeviantArt</td>
<td>Allowed</td>
<td>367.91 MB</td>
<td>1,375</td>
</tr>
<tr>
<td>6</td>
<td>XING</td>
<td>Allowed</td>
<td>264.08 MB</td>
<td>3,621</td>
</tr>
<tr>
<td>7</td>
<td>LinkedIn</td>
<td>Allowed</td>
<td>101.10 MB</td>
<td>5,462</td>
</tr>
<tr>
<td>8</td>
<td>Pinterest</td>
<td>Allowed</td>
<td>28.27 MB</td>
<td>1,476</td>
</tr>
<tr>
<td>9</td>
<td>Tinder</td>
<td>Allowed</td>
<td>24.05 MB</td>
<td>99</td>
</tr>
<tr>
<td>10</td>
<td>Jodel</td>
<td>Allowed</td>
<td>12.81 MB</td>
<td>830</td>
</tr>
<tr>
<td>11</td>
<td>Yammer</td>
<td>Allowed</td>
<td>11.01 MB</td>
<td>1,724</td>
</tr>
<tr>
<td>12</td>
<td>Snapchat</td>
<td>Allowed</td>
<td>9.70 MB</td>
<td>961</td>
</tr>
<tr>
<td>13</td>
<td>Google.Plus</td>
<td>Allowed</td>
<td>3.43 MB</td>
<td>147</td>
</tr>
<tr>
<td>14</td>
<td>Ning</td>
<td>Allowed</td>
<td>1.43 MB</td>
<td>24</td>
</tr>
<tr>
<td>15</td>
<td>Google.Groups</td>
<td>Allowed</td>
<td>906.58 KB</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>Flickr</td>
<td>Allowed</td>
<td>318.45 KB</td>
<td>14</td>
</tr>
<tr>
<td>17</td>
<td>Foursquare</td>
<td>Allowed</td>
<td>173.66 KB</td>
<td>13</td>
</tr>
<tr>
<td>18</td>
<td>Vkontakte</td>
<td>Allowed</td>
<td>135.23 KB</td>
<td>27</td>
</tr>
<tr>
<td>19</td>
<td>Reddit</td>
<td>Allowed</td>
<td>60.28 KB</td>
<td>15</td>
</tr>
<tr>
<td>20</td>
<td>Tapatalk</td>
<td>Allowed</td>
<td>54.80 KB</td>
<td>2</td>
</tr>
</tbody>
</table>
### Top-Video-/Audio-Streaming-Anwendungen

<table>
<thead>
<tr>
<th>#</th>
<th>Application</th>
<th>Action</th>
<th>Bandwidth</th>
<th>Session Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>YouTube</td>
<td>Allowed</td>
<td>75.13 GB</td>
<td>68.039</td>
</tr>
<tr>
<td>2</td>
<td>HTTP:Video</td>
<td>Allowed</td>
<td>23.90 GB</td>
<td>2.683</td>
</tr>
<tr>
<td>3</td>
<td>Spotify</td>
<td>Allowed</td>
<td>3.29 GB</td>
<td>3.375</td>
</tr>
<tr>
<td>4</td>
<td>Dailymotion</td>
<td>Allowed</td>
<td>2.21 GB</td>
<td>556</td>
</tr>
<tr>
<td>5</td>
<td>iTunes_Select.Play</td>
<td>Allowed</td>
<td>580.75 MB</td>
<td>198</td>
</tr>
<tr>
<td>6</td>
<td>Vimeo</td>
<td>Allowed</td>
<td>273.48 MB</td>
<td>796</td>
</tr>
<tr>
<td>7</td>
<td>Ooyala</td>
<td>Allowed</td>
<td>197.83 MB</td>
<td>100</td>
</tr>
<tr>
<td>8</td>
<td>HTTP:Audio</td>
<td>Allowed</td>
<td>62.41 MB</td>
<td>44</td>
</tr>
<tr>
<td>9</td>
<td>Deezer</td>
<td>Allowed</td>
<td>52.31 MB</td>
<td>156</td>
</tr>
<tr>
<td>10</td>
<td>CNN:Video</td>
<td>Allowed</td>
<td>51.53 MB</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>Amazon:Video</td>
<td>Allowed</td>
<td>36.25 MB</td>
<td>2.771</td>
</tr>
<tr>
<td>12</td>
<td>SoundCloud</td>
<td>Allowed</td>
<td>17.99 MB</td>
<td>1.319</td>
</tr>
<tr>
<td>13</td>
<td>RTCP</td>
<td>Allowed</td>
<td>11.70 MB</td>
<td>519</td>
</tr>
<tr>
<td>14</td>
<td>Last.FM</td>
<td>Allowed</td>
<td>8.68 MB</td>
<td>372</td>
</tr>
<tr>
<td>15</td>
<td>Netflix</td>
<td>Allowed</td>
<td>6.48 MB</td>
<td>381</td>
</tr>
<tr>
<td>16</td>
<td>Flowplayer</td>
<td>Allowed</td>
<td>1.19 MB</td>
<td>18</td>
</tr>
<tr>
<td>17</td>
<td>RTMPE</td>
<td>Allowed</td>
<td>1.002.60 KB</td>
<td>5</td>
</tr>
<tr>
<td>18</td>
<td>Twitch</td>
<td>Allowed</td>
<td>843.37 KB</td>
<td>27</td>
</tr>
<tr>
<td>19</td>
<td>Zune</td>
<td>Allowed</td>
<td>674.74 KB</td>
<td>7</td>
</tr>
<tr>
<td>20</td>
<td>Shazam</td>
<td>Allowed</td>
<td>439.76 KB</td>
<td>28</td>
</tr>
</tbody>
</table>

### Top-Spieleanwendungen

<table>
<thead>
<tr>
<th>#</th>
<th>Application</th>
<th>Action</th>
<th>Bandwidth</th>
<th>Session Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Steam</td>
<td>Allowed</td>
<td>38.69 MB</td>
<td>53</td>
</tr>
<tr>
<td>2</td>
<td>Clash.Of.Clans</td>
<td>Allowed</td>
<td>3.93 MB</td>
<td>32</td>
</tr>
<tr>
<td>3</td>
<td>Apple.Game.Center</td>
<td>Allowed</td>
<td>3.55 MB</td>
<td>662</td>
</tr>
<tr>
<td>4</td>
<td>Playstation.Network</td>
<td>Allowed</td>
<td>2.06 MB</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Super.Mario.Run</td>
<td>Allowed</td>
<td>257.05 KB</td>
<td>47</td>
</tr>
<tr>
<td>6</td>
<td>Madden.NFL.Mobile</td>
<td>Allowed</td>
<td>80.60 KB</td>
<td>16</td>
</tr>
<tr>
<td>7</td>
<td>Valve.Games</td>
<td>Allowed</td>
<td>11.36 KB</td>
<td>170</td>
</tr>
<tr>
<td>8</td>
<td>Warcraft</td>
<td>Allowed</td>
<td>6.04 KB</td>
<td>34</td>
</tr>
<tr>
<td>9</td>
<td>Xbox</td>
<td>Allowed</td>
<td>2.72 KB</td>
<td>2</td>
</tr>
</tbody>
</table>

### Top-Peer-to-Peer-Anwendungen

<table>
<thead>
<tr>
<th>#</th>
<th>Application</th>
<th>Action</th>
<th>Bandwidth</th>
<th>Session Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BitTorrent</td>
<td>Allowed</td>
<td>6.71 KB</td>
<td>77</td>
</tr>
<tr>
<td>2</td>
<td>Bitcomet:HTTP.Seed</td>
<td>Allowed</td>
<td>2.53 KB</td>
<td>162</td>
</tr>
</tbody>
</table>
# Webnutzung

## Top-Webkategorien

<table>
<thead>
<tr>
<th>#</th>
<th>Category</th>
<th>Browsing Time (hh:mm:ss)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information Technology</td>
<td>463:20:40</td>
</tr>
<tr>
<td>2</td>
<td>Search Engines and Portals</td>
<td>169:47:36</td>
</tr>
<tr>
<td>3</td>
<td>News and Media</td>
<td>123:28:16</td>
</tr>
<tr>
<td>4</td>
<td>Business</td>
<td>123:24:40</td>
</tr>
<tr>
<td>5</td>
<td>Information and Computer Security</td>
<td>78:11:13</td>
</tr>
<tr>
<td>6</td>
<td>Social Networking</td>
<td>45:42:40</td>
</tr>
<tr>
<td>7</td>
<td>Shopping</td>
<td>32:59:27</td>
</tr>
<tr>
<td>8</td>
<td>Reference</td>
<td>25:56:50</td>
</tr>
<tr>
<td>9</td>
<td>Real Estate</td>
<td>20:09:43</td>
</tr>
<tr>
<td>10</td>
<td>Games</td>
<td>17:39:54</td>
</tr>
</tbody>
</table>

## Top-Webanwendungen

<table>
<thead>
<tr>
<th>#</th>
<th>Risk</th>
<th>Web Application</th>
<th>Technology</th>
<th>User</th>
<th>Bandwidth</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>HTTPS.BROWSER</td>
<td>Browser-Based</td>
<td>191</td>
<td>81.96 GB</td>
<td>1,877,833</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>Microsoft.Outlook</td>
<td>Browser-Based</td>
<td>119</td>
<td>76.94 GB</td>
<td>881,280</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>YouTube</td>
<td>Browser-Based</td>
<td>133</td>
<td>75.11 GB</td>
<td>67,400</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>MS.Windows.Update</td>
<td>Client-Server</td>
<td>115</td>
<td>31.66 GB</td>
<td>100,461</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>HTTP.Video</td>
<td>Browser-Based</td>
<td>46</td>
<td>23.90 GB</td>
<td>2,683</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>HTTP.Download.Accelerator</td>
<td>Browser-Based</td>
<td>96</td>
<td>21.44 GB</td>
<td>5,446</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>Microsoft.Portrait</td>
<td>Browser-Based</td>
<td>148</td>
<td>18.88 GB</td>
<td>159,845</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>HTTP.BROWSER</td>
<td>Browser-Based</td>
<td>253</td>
<td>15.35 GB</td>
<td>639,361</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>Google.Services</td>
<td>Browser-Based</td>
<td>176</td>
<td>14.99 GB</td>
<td>287,163</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>HTTP.Segmented.Download</td>
<td>Browser-Based</td>
<td>122</td>
<td>14.28 GB</td>
<td>3,652</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>Apple.Services</td>
<td>Client-Server</td>
<td>86</td>
<td>13.39 GB</td>
<td>25,160</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>HTTP.BROWSER_Firefox</td>
<td>Browser-Based</td>
<td>81</td>
<td>12.23 GB</td>
<td>341,795</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>Facebook</td>
<td>Browser-Based</td>
<td>149</td>
<td>10.70 GB</td>
<td>84,854</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>HTTP.BROWSER_Chrome</td>
<td>Browser-Based</td>
<td>105</td>
<td>8.37 GB</td>
<td>193,315</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>Amazon.Services</td>
<td>Browser-Based</td>
<td>114</td>
<td>6.68 GB</td>
<td>103,195</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>Instagram</td>
<td>Client-Server</td>
<td>69</td>
<td>6.15 GB</td>
<td>12,186</td>
</tr>
<tr>
<td>17</td>
<td>3</td>
<td>SSL_TLSv1.2</td>
<td>Network-Protocol</td>
<td>110</td>
<td>4.57 GB</td>
<td>63,804</td>
</tr>
<tr>
<td>18</td>
<td>2</td>
<td>Microsoft.Office.Update</td>
<td>Client-Server</td>
<td>37</td>
<td>3.69 GB</td>
<td>3,519</td>
</tr>
<tr>
<td>19</td>
<td>2</td>
<td>Spotify</td>
<td>Client-Server</td>
<td>34</td>
<td>3.27 GB</td>
<td>3,094</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>Apple.Software.Update</td>
<td>Client-Server</td>
<td>27</td>
<td>2.80 GB</td>
<td>2,917</td>
</tr>
<tr>
<td>#</td>
<td>Website</td>
<td>Category</td>
<td>Requests</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>------------------------------</td>
<td>---------------------------</td>
<td>-----------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>http.00.a.sophosxi.net</td>
<td>Information Technology</td>
<td>1,405,163</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>d1.sophosudp.com</td>
<td>Information and Computer Security</td>
<td>92,758</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>clients3.google.com</td>
<td>Search Engines and Portals</td>
<td>87,797</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>dci.sophosudp.com</td>
<td>Information Technology</td>
<td>77,005</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>http.00.s.sophosxi.net</td>
<td>Information and Computer Security</td>
<td>67,616</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>dci.sophosudp.net</td>
<td>Information Technology</td>
<td>64,848</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>resolver1.ast.ctmail.com</td>
<td>Information Technology</td>
<td>58,328</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>netsrv11.tik.net</td>
<td>Domain Parking</td>
<td>57,330</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>d2.sophosudp.com</td>
<td>Information Technology</td>
<td>49,320</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>bilder.bild.de</td>
<td>News and Media</td>
<td>47,585</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>detectportal.firefox.com</td>
<td>Information Technology</td>
<td>46,383</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>citrixweb</td>
<td>Unrated</td>
<td>42,411</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>crl.microsoft.com</td>
<td>Information Technology</td>
<td>39,916</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>pagead2.google.syndication.com</td>
<td>Advertising</td>
<td>33,251</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>10.8.1.235:3910</td>
<td>Unrated</td>
<td>28,816</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td><a href="http://www.exclusive-networks.com">www.exclusive-networks.com</a></td>
<td>Information Technology</td>
<td>27,048</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>ocsp.digicert.com</td>
<td>Information Technology</td>
<td>26,024</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>ww251.smartadserver.com</td>
<td>Advertising</td>
<td>25,268</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>officecdn.microsoft.com.edgesuite.net</td>
<td>Information Technology</td>
<td>24,372</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>ib.adnxs.com</td>
<td>Advertising</td>
<td>23,870</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Meist besuchte Webdomänen nach Surfzeit

<table>
<thead>
<tr>
<th>#</th>
<th>Sites</th>
<th>Category</th>
<th>Browsing Time (hh:mm:ss)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>resolver1.ast.ctmail.com</td>
<td>Information Technology</td>
<td>308:09:48</td>
</tr>
<tr>
<td>2</td>
<td>http.00.a.sophosxl.net</td>
<td>Information Technology</td>
<td>199:02:30</td>
</tr>
<tr>
<td>3</td>
<td>detectportal.firefox.com</td>
<td>Information Technology</td>
<td>192:40:46</td>
</tr>
<tr>
<td>4</td>
<td>crl.microsoft.com</td>
<td>Information Technology</td>
<td>98:58:20</td>
</tr>
<tr>
<td>5</td>
<td>ocsp.digicert.com</td>
<td>Information Technology</td>
<td>89:52:12</td>
</tr>
<tr>
<td>6</td>
<td><a href="http://www.microsoft.com">www.microsoft.com</a></td>
<td>Information Technology</td>
<td>86:51:24</td>
</tr>
<tr>
<td>7</td>
<td>clients1.google.com</td>
<td>Search Engines and Portals</td>
<td>70:28:49</td>
</tr>
<tr>
<td>8</td>
<td><a href="http://www.bild.de">www.bild.de</a></td>
<td>News and Media</td>
<td>68:44:53</td>
</tr>
<tr>
<td>9</td>
<td>http.00.s.sophosxl.net</td>
<td>Information and Computer Security</td>
<td>60:15:10</td>
</tr>
<tr>
<td>10</td>
<td>crl.swissign.net</td>
<td>Information Technology</td>
<td>55:39:35</td>
</tr>
<tr>
<td>11</td>
<td>ping.chartbeat.net</td>
<td>Information Technology</td>
<td>55:32:53</td>
</tr>
<tr>
<td>12</td>
<td>clients3.google.com</td>
<td>Search Engines and Portals</td>
<td>53:09:22</td>
</tr>
<tr>
<td>13</td>
<td>getgreenshot.org</td>
<td>Information Technology</td>
<td>50:24:39</td>
</tr>
<tr>
<td>14</td>
<td>ups.xplosion.de</td>
<td>Business</td>
<td>47:10:09</td>
</tr>
<tr>
<td>15</td>
<td>ss.symcd.com</td>
<td>Information Technology</td>
<td>43:32:25</td>
</tr>
<tr>
<td>16</td>
<td>wetter.bild.de</td>
<td>News and Media</td>
<td>39:26:07</td>
</tr>
<tr>
<td>17</td>
<td>cdn.content.prod.cms.msn.com</td>
<td>Search Engines and Portals</td>
<td>36:30:47</td>
</tr>
<tr>
<td>18</td>
<td>bilder.bild.de</td>
<td>News and Media</td>
<td>33:46:51</td>
</tr>
<tr>
<td>19</td>
<td>ocs.p2.globalsign.com</td>
<td>Information Technology</td>
<td>30:09:51</td>
</tr>
<tr>
<td>20</td>
<td>odb.outbrain.com</td>
<td>Business</td>
<td>28:26:46</td>
</tr>
</tbody>
</table>
Netzwerknutzung

Nachfolgend zur Übersicht und zum besseren Verständnis eine Übersicht des analysierten Datenverkehrs. Diese Daten sollen Sie insbesondere bei der Planung weiterer Maßnahmen unterstützen, da sie wichtige Kriterien wie Anzahl der Sessions, Bandbreite, Anzahl der Benutzer, etc. aufzeigen.

<table>
<thead>
<tr>
<th># Zusammenfassung</th>
<th>Werte</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Total Sessions</td>
<td>27,328,903</td>
</tr>
<tr>
<td>2 Total Bytes Transferred</td>
<td>532.60GB</td>
</tr>
<tr>
<td>3 Most Active Date By Sessions</td>
<td>2017-04-26</td>
</tr>
<tr>
<td>4 Total Users</td>
<td>256,235</td>
</tr>
<tr>
<td>5 Total Applications</td>
<td>16,266</td>
</tr>
<tr>
<td>6 Total Destinations</td>
<td>59,636</td>
</tr>
<tr>
<td>7 Average Sessions Per Day</td>
<td>910,963</td>
</tr>
<tr>
<td>8 Average Bytes Per Day</td>
<td>17.75GB</td>
</tr>
</tbody>
</table>

Bandbreitenschöpfende-Top-Quellen/-Ziele

<table>
<thead>
<tr>
<th># Hostname(or IP)</th>
<th>Bandwidth</th>
<th>Sent</th>
<th>Received</th>
<th>Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 microsoft.com</td>
<td>15.71 GB</td>
<td></td>
<td></td>
<td>46,061</td>
</tr>
<tr>
<td>3 giomex.com</td>
<td>15.18 GB</td>
<td></td>
<td></td>
<td>2,022</td>
</tr>
<tr>
<td>4 apple.com</td>
<td>14.70 GB</td>
<td></td>
<td></td>
<td>7,590</td>
</tr>
<tr>
<td>5 windowsupdate.com</td>
<td>14.61 GB</td>
<td></td>
<td></td>
<td>6,519</td>
</tr>
<tr>
<td>6</td>
<td>11.40 GB</td>
<td></td>
<td></td>
<td>618,931</td>
</tr>
<tr>
<td>7</td>
<td>11.02 GB</td>
<td></td>
<td></td>
<td>102,628</td>
</tr>
<tr>
<td>8</td>
<td>9.80 GB</td>
<td></td>
<td></td>
<td>358</td>
</tr>
<tr>
<td>9</td>
<td>8.84 GB</td>
<td></td>
<td></td>
<td>17,171</td>
</tr>
<tr>
<td>10</td>
<td>4.77 GB</td>
<td></td>
<td></td>
<td>4,365,782</td>
</tr>
<tr>
<td>11 cloudfront.net</td>
<td>4.74 GB</td>
<td></td>
<td></td>
<td>1,722</td>
</tr>
<tr>
<td>12 edgesuite.net</td>
<td>4.03 GB</td>
<td></td>
<td></td>
<td>1,882</td>
</tr>
<tr>
<td>13</td>
<td>3.73 GB</td>
<td></td>
<td></td>
<td>637,408</td>
</tr>
<tr>
<td>14</td>
<td>3.37 GB</td>
<td></td>
<td></td>
<td>44,529</td>
</tr>
<tr>
<td>15</td>
<td>3.25 GB</td>
<td></td>
<td></td>
<td>157,073</td>
</tr>
<tr>
<td>16</td>
<td>3.22 GB</td>
<td></td>
<td></td>
<td>46,073</td>
</tr>
<tr>
<td>17</td>
<td>3.06 GB</td>
<td></td>
<td></td>
<td>37,915</td>
</tr>
<tr>
<td>18</td>
<td>3.04 GB</td>
<td></td>
<td></td>
<td>30,312</td>
</tr>
<tr>
<td>19</td>
<td>3.03 GB</td>
<td></td>
<td></td>
<td>36,651</td>
</tr>
<tr>
<td>20</td>
<td>3.03 GB</td>
<td></td>
<td></td>
<td>45,328</td>
</tr>
</tbody>
</table>
Übersicht über das Sessionaufkommen während des ECTAs

Aktive Benutzer
Appendix A

Devices

ECTA-FortiGate[ECTA]