DEUTSCHLANDS UNABHÄNGIGES MAGAZIN FÜR ANLAGEBERATER
FONDS professionell ONLINE

27.07.2018 | Unternehmen

Cyber-Attacken: Sieben Tipps, wie sich Firmen schützen können

Wannacry, Petya, Operation Shady Rat. Die Zahl der Cyber-Attacken ist in den letzten Jahren massiv gestiegen. Sieben Tipps, wie Sie sich richtig vor unliebsamen Angriffen schützen, haben die IT-Experten von Iphos IT Solutions zusammengetragen.

Hier erfahren Sie, wie Sie sich am besten vor Cyber-Attacken schützen – **einfach weiterklicken!**

Foto: © Jakub Krechowicz / stock.adobe.com

1. Nicht nur das Virenprogramm updaten!
Eigentlich sollten regelmäßige Updates selbstverständlich sein. Doch als Wannacry eine Microsoft-Sicherheitslücke für Angriffe nutzte, hatte das Unternehmen 59 Tage nachdem Wannacry erstmals aufgetaucht war, ein Sicherheitsupdate herausgegeben. Die Installation dieses Updates hätte die rasante Ausbreitung auf über 220.000 infizierten Computern in über 150 Ländern innerhalb von nur drei Tagen verhindert.

Nur das Virenprogramm auf den neuesten Stand zu halten, genügt deshalb schlicht nicht. Die Updates für Software, Betriebssysteme und Firewall sollten immer regelmäßig und rasch installiert werden, mahnt Iphos IT Solutions. Wie das Beispiel von Wannacry zeigt, ist ein effizientes Patchmanagement einer der wichtigsten Schritte in Richtung IT-Sicherheit und Schutz vor Cybercrime.

Foto: © Mathias Rosenthal / stock.adobe.com

2. Wenn die eigenen Mitarbeiter zur Gefahr werden
Doch Gefahr droht nicht nur von außen. In den meisten Fällen wird Malware von Mitarbeitern durch unbedachtes Öffnen von E-Mail Anhängen, Folgen von Hyperlinks, privatem Surfverhalten oder mittels externer Medien, wie etwa USB-Sticks, in das Unternehmensnetzwerk eingeschleust.

Eine aktuelle Antivirus-Software soll zwar vor Malware-Angriffen schützen, jedoch sei diese oder eine zusätzliche Security-Software nicht immer der Weisheit letzter Schluss, betont Iphos IT Solutions. Wenn von IT-Security gesprochen wird, denken viele nur an technische, produktorientierte Lösungen. Man sollte aber unbedingt auch das Bewusstsein der eigenen Mitarbeiter dahingehend schärfen.

Foto: © Production Perig / stock.adobe.com

3. Die richtige Backup-Strategie
Hat sich ein Unternehmen trotz Security Maßnahmen einen Verschlüsselungstrojaner eingefangen, sollte man besser auf eine umfassende Backup-Strategie gesetzt haben. Dazu gehören zum Beispiel gespiegelte, sich gegenseitig überwachende Server-Systeme und tägliche Sicherungen, die offline – also außerhalb der Zugriffsmöglichkeit von Ransomware – aufbewahrt werden.

Foto: © bizoo_n / stock.adobe.com

4. Passwort-Regelungen
Passwörter, die aus einfachen Zahlenkombinationen oder persönlichen Informationen bestehen, sollten inzwischen tabu sein. Iphos IT Solutions rät darüber hinaus zu klaren Regeln bezüglich der Passwort-Generierung und auch der Aufbewahrung. Außerdem sollten die Passwörter regelmäßig geändert werden. Zur Verwaltung der Passwörter eignet sich die Verwendung eines Passwort-Safes.

Foto: © designer491 / stock.adobe.com

5. Für alle Fälle: Checklisten erstellen
Prozesse und Checklisten sollten ebenso Bestandteil einer IT-Strategie sein. Genau festzuhalten, was im Falle eines Falles zu tun ist, spart Zeit und kann helfen, das Schlimmste zu verhindern oder Folgeschäden zu minimieren. Egal ob es sich um Cyber-Angriffe oder andere IT-Vorfälle handelt, eine "Desaster Recovery Strategie" mit zuvor festgelegten und getesteten Prozessen ist von essentieller Bedeutung, betont Iphos IT Solutions.

Foto: © Sensay / stock.adobe.com

6. Den Internetdienstanbieter nicht vergessen!
Aber auch an den Internetanbieter sollte gedacht werden. Denn sogenannte DDoS-Angriffe richten sich meist gegen Web-, Mail oder DNS-Server. Bei solchen Attacken wird mehr Datenverkehr auf bestimmte IP-Adressen umgeleitet als diese verarbeiten kann – bis der Server kracht. Unternehmen sollten daher darauf achten, dass der Internetdienstanbieter den Datenverkehr im Backbone (hier bündeln sich die Daten aller Endbenutzer) des Netzes überwacht und bei auffälligen Abweichungen eingreift. Für den Fall, dass es zu einer Attacke kommt, sollten auch gemeinsam mit dem Provider entsprechende Prozesse und Checklisten erstellt werden.

Foto: © wladimir1804 / stock.adobe.com

7. Risikomanagement nicht unterschätzen
Spätestens seit der im Mai in Kraft getretenen Datenschutzverordnung ist bekannt: In einer sauber geführten IT-Landschaft darf eine Risiko-Analyse hinsichtlich der Unternehmens-IT nicht fehlen. Denn gerade bei Cyber-Angriffen ist können sensible, personenbezogene Daten geklaut werden. Wenn dann doch einmal etwas passiert, sei man laut Iphos IT Solutions mit einer Risiko-Analyse und einer Strategie zur Schadensbegrenzung gut abgesichert.

Foto: © Gajus / stock.adobe.com

Nicht nur Banken, Versicherungen oder Fondsgesellschaften sollten sich gut vor Cyber-Attaken schützen. Spätestens seit Inkrafttretten der neuen EU-Datenschutzgrundverordnung (DSGVO) sollten auch Berater ihre IT-Systeme aufgerüstet haben. Denn nicht selten haben es Kriminelle auf hochsensible Daten abgesehen. Zudem sind Angriffe auf die IT-Infrastruktur von Unternehmen jeder Größe in den letzten Jahren ernorm gestiegen.

"Mitverantwortlich dafür ist die steigende Verbreitung von Ransomware", erklärt Manuel Kern, CTO bei Iphos IT Solutions. "Durch die dabei eingesetzten Kryptotrojaner werden Daten auf den befallenen Rechnern verschlüsselt und sind damit für die User nicht mehr nutzbar." Gegen ein Lösegeld (englisch: Ransom) versprechen die Täter dann die Übermittlung eines Schlüssels zur Wiederherstellung des Kundenkontos – ein Versprechen, das aber oft nicht gehalten wird. Verbreitet werden die Verschlüsselungstrojaner meist durch E-Mails, unsichere Downloads aus dem Internet sowie Sicherheitslücken in den verwendeten Web-Browsern und Betriebssystemen.

Ebenfalls auf die Verbreitung durch E-Mails setzen Cyberkriminelle bei ihren Phishing-Attacken. Durch zusehends besser gefälschte Nachrichten von Institutionen wie Banken, Online-Shops, werden User zu ebenfalls täuschend echt aussehenden Webportalen weitergeleitet, über die die Login-Daten ausspioniert werden. Aber auch Mails, in denen Betrüger sich als Vorgesetzten ausgeben und Zahlungen anordnen – Stichwort Social Engeneering –, sind immer häufiger an der Tagesordnung.

Wie sich Unternehmen gegen solche Cyber-Angriffe wehren können, **finden unsere Leser in der Bilderstrecke oben heraus!** *(cf)*