Die TOP 10 Gefahren im Internet – und wie Sie Ihr Unternehmen kinderleicht ruinieren

Handout zum Unternehmerdialog der Wirtschaftsjunioren Bonn/Rhein-Sieg am 28. August 2014 in der IHK Bonn/Rhein-Sieg

Allein in Deutschland werden jährlich über 200.000 Internetpräsenzen gehackt.

Der Schaden beschränkt sich nicht nur auf die Kosten der Desinfektion, sondern es entstehen Reputationsschäden und wirtschaftliche Folgeschäden. Es kann weiterhin zu rechtlichen Konsequenzen für Geschäftsführung und Datenschutzbeauftragte kommen. Besucher der Website und Kunden können zusätzlich betroffen sein.

Basisschutz lokal

Die Großzahl gehackter Websites und IT-Systeme ist darauf zurück zu führen, dass die regulären Zugangsdaten bei einem Einbruch in einen lokalen PC gestohlen wurden (Malware, Viren, Trojaner). Die Absicherung des eigenen, lokalen Arbeitsplatzes hat damit eine große Bedeutung:

- http://bit.ly/internetsicherheit01 bietet eine umfassende Anleitung für einen Basisschutz Ihres lokalen Arbeitsplatzes.
- Verwenden Sie einen Passworttresor für die Verwaltung Ihrer Passwörter (z.B. 1Password oder Keepass) und beachten Sie unbedingt die Hinweise zu sicheren Passwörtern auf http://bit.ly/internetsicherheit02.
- Sorgen Sie für Updates zeitnah nach dem Erscheinen. Nicht nur Betriebssystem (Windows/Mac/Linux), Browser und Antivirus-Programm, sondern auch für Ihren Router (FritzBox o.ä.).

Sicherheitswarnungen und Infos zu wichtigen Updates sollte man beim Bürger-CERT (CERT = Computer Emergency Response Team) des BSI abonnieren:
http://bit.ly/internetsicherheit05

Basisschutz unterwegs

Ein weiterer Angriffsvektor ist das Mithören von Verbindungen, wenn Sie über öffentliche Hotspots und WLANs mit dem Internet verbunden sind (Zug, Hotel, Restaurant, …). Das Mitschneiden ist hier nicht weiter schwer. Ein Auslesen von Zugangsdaten (nicht nur zum Webserver, auch zu GMX, GMail, etc) oder ein Übernehmen Ihrer aktuellen Sitzung ist kein größeres Problem.

- Verwenden Sie für Ihr Smartphone und Ihren Laptop ausschließlich gesicherte Verbindungen über ein VPN. VPN mit FritzBox einrichten: http://bit.ly/internetsicherheit08
- Verschlüsseln Sie die Daten auf Ihrem Smartphone und Ihrem Laptop und lassen Sie beides auf keinen Fall unbeaufsichtigt.
- Verwenden Sie Ihr Smartphone auf keinen Fall für Banking, das Speichern von Zugangsdaten oder für den Zugang zu sensiblen Systemen.
- Beachten Sie die Hinweise auf http://bit.ly/internetsicherheit04

Sensibilisierungsschulung Ihrer Mitarbeiter

Ein Basisschutz kann in den meisten Punkten technisch realisiert werden, so dass Mitarbeiter ohne weitere Kenntnisse gegen die meisten, unspezifischen Angriffe geschützt sind. Anders sieht dies jedoch bei spezifischen, zielgerichteten Angriffen gegen Ihr Unternehmen aus.

Motivation Ihr Unternehmen zielgerichtet anzugreifen sind zum Beispiel (Schutzgeld-) Erpressung, Datendiebstahl oder Wirtschaftsspionage, Schädigung durch Konkurrenten.

Diese Angriffe laufen selten mit rein technischen Mitteln. Ein “Social Engineering”, also die Manipulation von Mitarbeitern ist sehr viel einfacher und erfolgsversprechender. Insbesondere dann, wenn Mitarbeiter nicht für diese Gefahr sensibilisiert wurden.

Basisschutz Webserver

Insbesondere für bekannte Sicherheitslücken gibt es Exploits (Programme, die diese Lücken auszunützen wissen und einen einfachen Einbruch ermöglichen). Angriffe werden inzwischen automatisiert durchgeführt, wobei ein Webserver innerhalb von Minuten mit Exploits attackiert wird. Fehlen Sicherheitsupdates und ist der Webserver nicht ordentlich gewartet, so ist der Angriff erfolgreich.

Vorbeugender Basis-Schutz

- Erkundigen Sie sich bei Ihrem Hoster, wie der eigentliche Server gewartet und mit Sicherheitsupdates versorgt wird.
- In der Regel werden für Websites heute Content-Management-Systeme genutzt (TYPO3, Wordpress, Drupal, Joomla, Sitecore, …), die nicht vom Hoster gewartet werden, sondern von Ihrem Dienstleister installiert wurden. Schliessen Sie mit Ihrem Internet-Dienstleister (Web- oder Werbeagentur) unbedingt einen Servicevertrag ab, der mindestens zeitnahe Sicherheitsupdates für diese Systeme und nach Möglichkeit auch ein Angriffsmonitoring (Intrusion Detection System und/oder Web Application Firewall) beinhaltet.
- Vermeiden Sie nach Möglichkeit die Notwendigkeit von FTP-Zugängen. Moderne Systeme erlauben Redakteuren das Übertragen von Bildern und Dateien auch ohne FTP.
- Wenn Sie FTP nutzen, dann ausschließlich die verschlüsselte Variante SFTP.

Benachrichtigung

Wenn Ihr System gehackt ist, gilt es schnell zu reagieren, die Website sofort offline zu nehmen und durch eine Wartungsmeldung zu ersetzen. Folgende freien Dienste helfen Ihnen, einen Hack zu erkennen und Sie zu benachrichtigen:

- Initiative S von BSI und eco http://bit.ly/internetsicherheit06
- Webmastertools von Google http://bit.ly/internetsicherheit07

Wenn es dann doch einmal passiert ist: Erste-Hilfe-Maßnahmen

Sie erfahren, dass Ihre Website gehackt ist. Von Initiative S, den Google Webmastertools oder von einem Kunden, der Ihnen erzählt, er bekomme eine Warnmeldung, wenn er auf Ihre Internetseite surft. Was nun?

1. Der Webserver muss sofort vom Netz. Ihr Provider hilft Ihnen dabei, den Server offline zu schalten und durch eine Wartungsmeldung zu ersetzen.
2. Führen Sie auf Ihrem lokalen Rechner eine Virendiagnose durch. Aktualisieren Sie zuvor die Virusdefinitionen Ihrer Antivirus-Software.
3. Setzen Sie ALLE Passwörter des Servers neu oder deaktivieren Sie diese Zugänge.
4. Wenn Sie von Google benachrichtigt wurden oder Google bereits auf die Malware auf Ihrem Rechner aufmerksam wurde müssen Sie jetzt Google mitteilen, dass der Schadcode auf Ihrer Website entfernt worden ist. Google prüft das und deaktiviert die Warnung für Besucher Ihrer Website. Auch verlieren Sie Trust und Ranking, wenn Sie nicht umgehend reagieren und Google über die Beseitigung der Gefahr informieren.

Jetzt geht es darum, auch die Manipulationen auf Ihrem Webserver zu desinfizieren, um die Website wieder live schalten zu können. Ab hier hilft nur die Unterstützung eines auf Desinfektion spezialisierten Profis:

1. Schadcode finden und entfernen.
2. Hintertüren finden und entfernen.
3. Schwachstelle, über die der Einbruch möglich war finden und entfernen.
4. Sicherheitsmonitoring aktivieren.

Der Referent

Peter Pröll ist Spezialist für TYPO3, Mitglied im TYPO3 Expert Advisory Board und Initiator der TYPO3 Sicherheitsinitative deutscher Internetagenturen. Zu seinen Kunden zählen die Vereinten Nationen, die XING AG, DIE ZEIT und die Stadt Bonn.

Neben der Beratung und Umsetzung von Internetprojekten bietet er Sicherheitsaudits und Sicherheitsberatung, sowie die Expertise zur Desinfektion erfolgter Hacks.

Kontakt: http://alinbu.net – peter@alinbu.net