Polizei

SAARLAND

Landespolizeipräsidium · Mainzer Straße 134-146. ·66121 Saarbrücken

Information der
Zentralen Ansprechstelle Cybercrime (ZAC)
des Landespolizeipräsidiums Saarland

Landespolizeipräsidium
LPP 2 Kriminalitätsbekämpfung/ Landeskriminalamt

Dezernat LPP 222

Dienst-gebäude: **Hellwigstraße 8-10**
66121 Saarbrücken

Bearbeiter_in: Schmitt M.O.KHK
Tel.: 0681 962 – 2431
Fax: 0681 962 –2445
E-Mail: cybercrime@polizei.slpol.de

Az: 34/2020

Datum: 10.07.2020

Welle von Erpresserschreiben über Kontaktformulare

Zurzeit werden vermehrt über Kontaktformulare auf Firmenwebseiten Erpresserschreiben versendet:

Betreff: Bitte leiten Sie diese E-Mail an jemanden in Ihrem Unternehmen weiter, der wichtige Entscheidungen treffen darf!

Stichworte: *Website, gehackt, extrahiert, Datenbank, Ruf, bitcoin*

Die Erpressernachricht ist im Gegensatz zu vorrausgegangen Erpressungswellen in deutscher Sprache verfasst. Die Wortwahl ist fast immer identisch. In nahezu allen Fällen dürfte es sich um vorgetäuschte Erpressungsversuche handeln, um die Angeschriebenen zur Zahlung zu veranlassen. In der Regel dürfte es in diesem Zusammenhang zu keinem Datenabfluss gekommen sein.

Die Polizei rät:

- Solchen Forderungen sollte niemals durch eine Zahlung nachkommen werden.
- Liegen in diesem Zusammenhang (Erpressungsschreiben) keine weiteren Hinweise auf einen Abfluss von Daten bei Ihnen vor, können Sie diese Nachricht problemlos löschen (als SPAM betrachten).
- Wenn Sie Anzeige erstatten möchten, suchen Sie Ihre örtliche Polizei-Dienststelle auf (*Pandemiebedingt bitte Termin vereinbaren*) oder nutzen Sie, die für Ihr Bundesland zuständige Onlinewache.

https://www.saarland.de/polizei/DE/onlinewache/onlinewache_node.html

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email: cybercrime@polizei.slpol.de

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Anlagen

Beispiel einer Erpresser Email.

Folgende Kundenanfrage wurde soeben über die Website versendet:
Name / Ansprechpartner: XXXXXX
E-Mail: XXXXX@XXXX.com

Betreff: Ihre Site wurde gehackt
Anfrage: Bitte leiten Sie diese E-Mail an jemanden in Ihrem Unternehmen weiter, der wichtige Entscheidungen treffen darf!

Wir haben Ihre Website http://www.XXX.de gehackt und Ihre Datenbanken extrahiert.

Wie ist es passiert?
Unser Team hat auf Ihrer Website eine Sicherheitslücke gefunden, die wir ausnutzen konnten. Nachdem wir die Sicherheitsanfälligkeit festgestellt hatten, konnten wir Ihre Datenbankanmeldeinformationen abrufen, Ihre gesamte Datenbank extrahieren und die Informationen auf einen Offshore-Server verschieben.

Was bedeutet das?

Wir werden systematisch eine Reihe von Schritten durchlaufen, um Ihren Ruf vollständig zu schädigen. Zuerst wird Ihre Datenbank durchgesickert oder an den Höchstbietenden verkauft, den er mit seinen Absichten verwendet. Wenn E-Mails gefunden werden, werden sie per E-Mail darüber informiert, dass ihre Informationen verkauft oder durchgesickert sind und Ihre Website http: //www.XXX.de einen Fehler begangen hat, wodurch Ihr Ruf geschädigt und verärgerte Kunden / Mitarbeiter mit allen verärgerten Personen konfrontiert wurden Kunden / Mitarbeiter tun. Schließlich werden alle Links, die Sie in den Suchmaschinen indiziert haben, basierend auf Blackhat-Techniken, die wir in der Vergangenheit verwendet haben, um unsere Ziele zu deindizieren, deindiziert.

Wie höre ich damit auf?

Wir sind bereit, den Ruf Ihrer Website gegen eine geringe Gebühr nicht zu zerstören. Die aktuelle Gebühr beträgt .322 BTC in Bitcoins (3000 USD).

Senden Sie das Bitcoin an die folgende Bitcoin-Adresse (Kopieren und Einfügen, da zwischen Groß- und Kleinschreibung unterschieden wird):

12WghuRH7b8K7mcJvxCzWQjW7RVEAC7qgx

Sobald Sie bezahlt haben, werden wir automatisch darüber informiert, dass es Ihre Zahlung war. Bitte beachten Sie, dass Sie die Zahlung innerhalb von 5 Tagen nach Erhalt dieser Mitteilung leisten müssen, da sonst das Datenbankleck, die versendeten E-Mails und die De-Indexierung Ihrer Website beginnen!

Wie bekomme ich Bitcoins?

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email: cybercrime@polizei.slpol.de
Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Sie können Bitcoins ganz einfach über mehrere Websites oder sogar offline an einem Bitcoin-Geldautomaten kaufen. Wir empfehlen Ihnen https://cex.io/ für den Kauf von Bitcoins.

Was ist, wenn ich nicht bezahle?

Wenn Sie sich entscheiden, nicht zu zahlen, starten wir den Angriff zum angegebenen Datum und halten ihn aufrecht, bis Sie dies tun. Es gibt keine Gegenmaßnahme dazu. Sie werden am Ende nur mehr Geld verschwenden, um eine Lösung zu finden. Wir werden Ihren Ruf bei Google und Ihren Kunden vollständig zerstören.

Dies ist kein Scherz. Antworten Sie nicht auf diese E-Mail. Versuchen Sie nicht, zu argumentieren oder zu verhandeln. Wir werden keine Antworten lesen. Sobald Sie bezahlt haben, werden wir aufhören, was wir getan haben und Sie werden nie wieder von uns hören!

Bitte beachten Sie, dass Bitcoin anonym ist und niemand herausfinden wird, dass Sie die Anforderungen erfüllt haben.

i.A.

M.O. Schmitt
Kriminalhauptkommissar

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email: cybercrime@polizei.slpol.de
Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html